UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Miha Ozimek

Podpora poslovnemu odločanju pri obvladovanju tveganj organizacije

MAGISTRSKO DELO

Mentor: prof. dr. Denis Trček

Ljubljana, 2016

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Večna pot 113
1000 Ljubljana, Slovenija
telefon: 01 47 98 100
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Številka: 148-MAG-ISO/2016
Datum: 29. 02. 2016

Miha OZIMEK, spec. inf. var.

Ljubljana

Fakulteta za računalništvo in informatiko Univerze v Ljubljani izdaja naslednjo magistrsko nalogo

Naslov naloge: **Podpora poslovnemu odločanju pri obvladovanju tveganj organizacije**

Support of business decision-making in risk management process

Tematika naloge:

Orodje za ocenjevanje tveganj je namenjeno pokrivanju ocenjevanja tveganj vseh področij v organizaciji, kjer bi deležniki (varnostni inženirji oziroma skrbniki sistemov vodenja, vodstvo, lastniki procesov oziroma vodje oddelkov, zaposleni in pogodbeni sodelavci, nadzorniki ter revizorji) na enostaven način prišli do izračuna tveganj, ki so možna v organizaciji in z njimi povezanimi ustreznimi ukrepi, ki jih organizacija izvaja z namenom zmanjševanja tveganj.
Kako to zagotoviti na pregleden in hkrati enostaven način? S programsko opremo, ki olajša delo ocenjevalcem, je možno oceniti vsa področja v organizaciji na tak način. Ker obstaja malo programske opreme, ki bi ocenjevalcem to omogočala v skladu z zakonodajo in hkrati dovolj preprosto, da ne bi bistveno obremenjevali poslovnih procesov, bi modularno pripravljena programska oprema pripomogla k bistveno boljšemu ocenjevanju tveganj, izvajanju ukrepov za izboljšave in s tem k boljšemu poslovanju organizacij. Cilj naloge je, da na podlagi zakonodaje in standardov prikaže metodološki pristop, ki se lahko realizira z ustrezno tržno naravnano programsko opremo. Le-ta pa lahko izboljša vodenje organizacije na področju obvladovanja tveganj.

Mentor:

prof. dr. Denis Trček

Fakulteta za računalništvo in informatiko
2
UNIVERZA V LJUBLJANI

Dekan:

prof. dr. Nikolaj Zimic

Zahvala

Za strokovno pomoč, usmerjanje in svetovanje pri izdelavi magistrskega dela se zahvaljujem mentorju prof. dr. Denisu Trčku. Za pomoč pri lektoriranju ter natančnem pregledu vsega zapisanega v tem delu se zahvaljujem svoji mami Jani Ozimek, prof. slov. Brez njiju in prof. dr. Igorja Beliča, ki je bil moj mentor pri diplomski in specialistični nalogi, to delo ne bi moglo biti izdelano kakovostno in celovito.

Hvala!

Posvetilo

Magistrsko delo posvečam svoji družini, ženi Saši, sinu Ožbeju in hčerki Zarji, ki so me podpirali, da sem svoj študij pripeljal do uspešnega zaključka.

Kazalo poglavij

Kazalo slik

Povzetek

Orodje za ocenjevanje tveganj je namenjeno pokrivanju ocenjevanja tveganj vseh področij v organizaciji, kjer bi deležniki (varnostni inženirji oziroma skrbniki sistemov vodenja, vodstvo, lastniki procesov oziroma vodje oddelkov, zaposleni in pogodbeni sodelavci, nadzorniki ter revizorji) na enostaven način prišli do izračuna tveganj, ki so možna v organizaciji in z njimi povezanimi ustreznimi ukrepi, ki jih organizacija izvaja z namenom zmanjševanja tveganj.

Kako to zagotoviti na pregleden in hkrati enostaven način? S programsko opremo, ki olajša delo ocenjevalcem, je možno oceniti vsa področja v organizaciji na tak način. Ker obstaja malo programske opreme, ki bi ocenjevalcem to omogočala v skladu z zakonodajo in hkrati dovolj preprosto, da ne bi bistveno obremenjevali poslovnih procesov, bi modularno pripravljena programska oprema pripomogla k bistveno boljšemu ocenjevanju tveganj, izvajanju ukrepov za izboljšave in s tem k boljšemu poslovanju organizacij. Cilj naloge je, da na podlagi zakonodaje in standardov prikaže metodološki pristop, ki se lahko realizira z ustrezno tržno naravnano programsko opremo. Le-ta pa lahko izboljša vodenje organizacije na področju obvladovanja tveganj.

Ključne besede: ocena tveganja, ukrepi za zmanjševanje tveganj, orodje za ocenjevanje tveganj, programska oprema, standardi, zakonodaja

Abstract

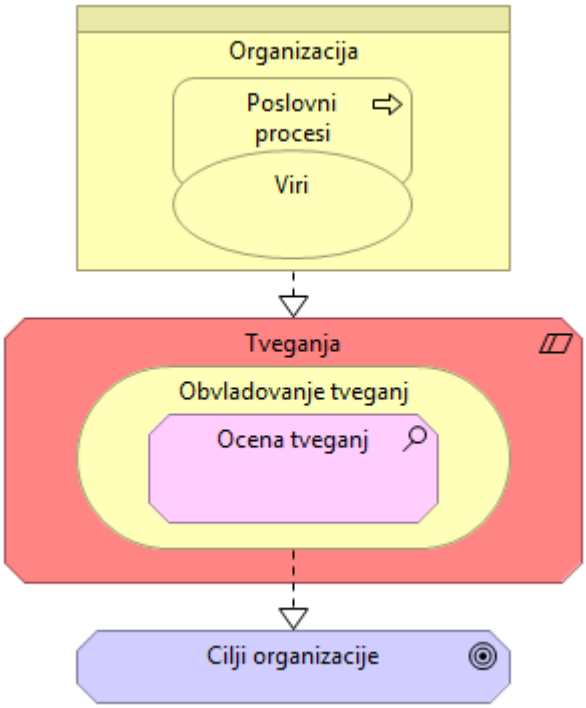
Tool for risk assessment is intended to cover the risk assessment of all areas of the organization where stakeholders - security engineers and management system administrators, management of the organization, process owners and heads of departments, employees and contract agents, supervisors, auditors, and others need an easy way to assess the risks that are possible in the organization and associated appropriate measures which are carried out by the organization in order to reduce these risks.

How to ensure a transparent and at the same time an easy way to assess the risk? With the software, which facilitates the work of the assessors, it is possible to assess all areas in the organization in a transparent and simple manner. Since there are very few examples of software that would allow assessors to carry out risk assessment in accordance with standards and legislation and that would be at the same time sufficiently simple not to cause substantial burden for key business processes owners, the modular architecture of software could help to improve risk assessment, implementation of measures for improvement and throughout this improve the business of the organization. Aim of the thesis is that on the basis of laws and standards methodological approach is prepared which is realized in the appropriate software tool that will improve the management of the organization in the segment of risk assessment.

Keywords: risk assessment, risk minimization measures, a tool for risk assessment, software, standards, legislation

1 Uvod

Programska oprema OTO, kar pomeni kratico za oceno tveganja organizacije, je namenjena obvladovanju tveganj različnim področjem v organizaciji, kjer bi vsi deležniki – varnostni inženirji oziroma skrbniki sistemov vodenja, vodstvo, lastniki procesov/vodje oddelkov, zaposleni/pogodbeni sodelavci, nadzorniki, revizorji, itd. na enostaven način prišli do vseh predpostavk tveganj, ki so možna v organizaciji in z njimi povezanimi ustreznimi ukrepi, ki jih organizacija izvaja z namenom zmanjševanja možnosti uresničitve teh tveganj. Programska oprema omogoča obvladovanje vseh vrst tveganj (ISO 31000) od tveganj poslovanja, varovanja informacij (ISO/IEC 27001, ZVOP, ZTP, ZVDAGA), neprekinjenega poslovanja (ISO 22301), kakovosti (ISO 9001), varstva pri delu (BS OHSAS 18001 oziroma ISO 45001), požarne varnosti, okoljskih ravnanj (ISO 14001) in ostalih. Na enem mestu tako pridemo do ustreznih ukrepov, ki izboljšujejo samo delovanje organizacije ter zmanjšujejo uresničitev tveganja na sprejemljivo raven.



Slika 1: Osnovni vidik ocenjevanja tveganja v programski opremi OTO

Tveganje, kot ga predstavlja standard ISO 31000, ki opredeljuje načela in smernice obvladovanja tveganja, je definirano kot vpliv negotovosti na doseganje ciljev poslovanja. Cilji poslovanja so v organizacijah seveda različni (poslovni, finančni, okoljski, varnostni), vpliv negotovosti pa naj bi pomenil pomanjkanje informacij o dogodkih, ki bi lahko vplivali na pričakovano doseganje ciljev poslovanja. Tveganje lahko izračunamo kot verjetnost posameznih dogodkov in posledic, ki jih ti dogodki prinašajo za doseganje ciljev organizacije. [1]

Ker je nemogoče natančno definirati verjetnost posameznih dogodkov in njihovih posledic, se vsaj z mehanizmom ocene tveganja poskuša čim bolj zavarovati organizacijo pred morebitno škodo, ki bi lahko nastala s samo uresničitvijo dogodkov.

Ocena tveganja tako predstavlja celovit proces identifikacije, ocene in ovrednotenja tveganj, ki organizacijam pomaga pri ustreznem upravljanju s tveganji z namenom ustvarjanja okolja, v katerem bi bilo poslovanje čim boljše. [1]

Identifikacija tveganja vključuje identifikacijo virov tveganja, dogodkov ter njihovih vzrokov in možnih posledic ter lahko vključuje pretekle podatke in potrebe deležnika. [1]

S pomočjo ocene tveganj, procesa, ki pomaga razumeti naravo tveganja in opredelitvijo ravni tveganja, poskuša organizacija oceniti posamezno tveganje z namenom kasnejšega ovrednotenja letega ter kasnejše ustrezne obravnave. [1]

Ovrednotenje tveganja je proces primerjave rezultatov ocene tveganj z merili tveganj z namenom, da se ugotovi, ali sta tveganje in/ali njegova velikost sprejemljiva oziroma dopustna. [1]

Z oceno tveganja opravimo ključni del obvladovanja tveganja in se pripravimo na ustrezno obravnavanje tveganja, ki je del odgovora na zagotavljanje ustreznega nivoja vodenja in izboljševanja poslovanja organizacije. Ocena tveganja postaja ključni element vseh sistemov vodenja in tega se vedno bolj zaveda tudi poslovodstvo organizacije, zato je primerna uvedba ocene tveganja v organizaciji ključni korak in bi moral biti opravljen v vseh organizacijah. S tem ne bomo zagotovili le skladnosti s standardi, ki opredeljujejo sisteme vodenja ali zakonodajo, ampak bomo vzpostavili mehanizem, ki naj bi organizacije pripeljal do večje 'odpornosti' na dogodke, ki škodljivo vplivajo na poslovanje.

1.1 Ocenjevanje tveganj v organizacijah

Ocenjevanje tveganj predstavlja za večino organizacij težavo, s katero se morajo spoprijeti, predvsem zaradi zahtev zakonodaje ali nadzornih organov, šele nato pa zaradi vodenja in izboljševanja samega poslovanja. S tega vidika je zato ocenjevanje tveganj trenutno predvsem administrativna naloga, ki mora biti opravljena, ne predstavlja pa še mehanizma, s pomočjo katerega bi organizacije vodile in izboljševale svoje poslovanje.

Prvi izziv za organizacijo, ki bi želela izkoristiti mehanizem ocene tveganja v celoti, je priprava okvirov, v katerih bi ta ocena tveganja delovala. Zavedati se je namreč potrebno, da je okolje, v katerem posluje organizacija, za vsako organizacijo drugačno, saj je potrebno pregledati vse izzive, s katerimi se organizacija sooča, da bi dosegla svoje cilje poslovanja. Že tukaj pa nastanejo težave, saj je potrebno za določanje okolja dobro poznati organizacijo, njen način poslovanja in cilje, h katerim teži.

Če predpostavljamo, da ima organizacija določene cilje in jasen način poslovanja, je potrebno definirati način oziroma tehnike ocenjevanja tveganj (metodologijo), po katerih se bo dalo tako kvantitativno kot kvalitativno ocenjevati tveganja, s pomočjo ocenjevanja pa priti do ustreznih ukrepov zmanjševanja tveganj. Poleg tega mora biti ocena tveganja ponovljiva, izvajana na enak način pri več različnih uporabnikih, enostavna in razumljiva, predstavljiva za nadzorne organe, inšpekcijske nadzore ter redno uporabljena. Vsi ti pogoji pa povzročajo težave izvajalcu ocenjevanja tveganj v organizaciji. Velikokrat se te kažejo kot nepremagljiva ovira za uspešno vzpostavitev mehanizma ocene tveganja v organizaciji.

Veliko organizacij zato nalogo ocenjevanja tveganj preda administrativnim službam, ki oceno tveganja pripravijo zgolj z vidika izpolnitve zahtev zakonodaje ali nadzornih organov. Pri tem je tovrstna ocena velikokrat neustrezna podlaga za pripravo učinkovitih ukrepov zmanjševanja tveganj, saj ne opredeljuje dejanskega stanja tveganj v organizaciji oziroma ne sledi poslovnim ciljem organizacije. Četudi je takšna ocena tveganja ponovljiva, ne izpolnjuje ostalih pogojev, kot so izvedba ocenjevanja pri več uporabnikih, enostavnost in razumljivost ter možnost predstavitve za nadzorne organe ali inšpekcijo.

Da bi se preprečilo neučinkovito ocenjevanje tveganj, je smiselno, če se organizacija ozre po dobrih praksah ocenjevanja tveganj, ki jih opredeljujejo standardi, in v proces celovitega obvladovanja tveganj (kamor spada tudi samo ocenjevanje) vključi poslovodstvo ter vodje organizacijskih enot oziroma skrbnike poslovnih procesov. Ker pa večje število izvajalcev ocenjevanja tveganj lahko predstavlja tudi več različnih pogledov na tveganja, je potrebno ocenjevanje tveganj vzpostaviti na enostaven in razumljiv način z ustreznimi kvantitativnimi in kvalitativnimi merili. Le tako lahko pričakujemo, da bodo vsi izvajalci ocenjevali na enak način in ustrezno. Ob tem bo ocena tveganja postala predstavljiva, ponovljiva in redno uporabljena.

V kolikor bo ocenjevanje tveganja v sklopu obvladovanja tveganja izvajano skladno z načeli obvladovanja tveganj, kakor jih opisuje standard ISO 31000, potem se lahko pričakuje, da bo organizacija med drugim:

- povečala verjetnost doseganja ciljev poslovanja,
- izboljšala vodenje organizacije,
- izboljšala zaupanje deležnikov,
- izboljšala delovno uspešnost in učinkovitost.

1.2 Načela obvladovanja (in s tem ocenjevanja) tveganj

Da bi bilo obvladovanje (in s tem ocenjevanje) tveganja uspešno, mora organizacija upoštevati naslednja načela obvladovanja tveganj, ki naj bi pripomogla, da:

- se ustvarja in varuje vrednost organizacije (prispeva k doseganju ciljev in izboljšanju poslovanja),
- je sestavni del vseh poslovnih procesov (ni samostojna aktivnost, ločena od procesov organizacije),
- je del odločanja poslovodstva (nosilci odločanja izbirajo na podlagi informacij in prednostno razvrščajo ukrepe),
- se izrecno obravnava negotovost (upošteva negotovost in njeno naravo),
- je sistematično, strukturirano in pravočasno (prispeva k učinkovitim, doslednim, primerljivim in zanesljivim rezultatom),
- temelji na najboljših razpoložljivih informacijah (pretekli podatki, izkušnje, povratne informacije deležnikov, opažanja, napovedi in strokovna presoja),
- je prilagojeno na okolje organizacije (notranje in zunanje okolje organizacije, profil tveganja),
- upošteva človeške in kulturne dejavnike (zmogljivosti, dojemanje in namere ljudi, ki omogočajo ali ovirajo doseganje ciljev),
- je pregledno in vključujoče (vključuje vse deležnike),
- je dinamično, ponovljivo in se odziva na spremembe (nenehno zaznavanje sprememb in ustrezen odziv nanje),
- se omogoča nenehno izboljševanje organizacije (razvijanje strategij za izboljšanje organizacije).

[1]

Iz samih načel obvladovanja tveganja se da razbrati, da je v sam proces obvladovanja tveganj nujno potrebno vključiti poslovodstvo organizacije, vse skrbnike procesov oziroma vodje organizacijskih enot ter jih vključiti v vsakodnevno poslovanje organizacije. Zato je moja predpostavka, da je odgovor na uspešno vpeljano obvladovanje (in s tem tudi ocenjevanje) tveganj treba iskati v vpeljavi ustrezne ocene tveganj za organizacijo in še bolj v avtomatizaciji in informatizaciji samega obvladovanja tveganj, ki omogočata hitro in učinkovito delo tudi s samo oceno tveganja.

1.3 Tehnike ocenjevanja tveganj

Tehnike ocenjevanja tveganj lahko najdemo v standardu ISO 31010, kjer so opisana naslednja orodja za ocenjevanje tveganj:

- iskanje idej oziroma viharjenje možganov (Brainstorming),
- strukturirani in polstrukturirani intervjuji (Structured or semi-structured interviews),
- tehnika Delphi (DELPHI),
- kontrolni seznami (Check-lists),
- primarna analiza tveganj (Primary hazard analysis),

- sistematične metode analize nevarnosti med obratovanjem HAZOP (Hazard and operability studies),
- analiza tveganja in ugotavljanja kritičnih kontrolnih točk HACCP (Hazard Analysis and Critical Control Points),
- ocena okoljskih tveganj (Environmental risk assessment),
- metoda SWIFT (Structure »What if«),
- analiza scenarija (Scenario analysis),
- analiza vpliva na poslovanje (Business impact analysis),
- analiza temeljnih vzrokov (Root cause analysis),
- sistematične metode analize odpovedi sistemov FMEA (Failure mode effect analysis),
- drevesna analiza okvar (Fault tree analysis)
- drevesna analiza dogodkov (Event tree analysis)
- analiza vzrokov in posledic (Cause and consequence analysis),
- analiza vzrokov in učinkov (Cause-and-effect analysis),
- analiza zaščitne ravni LOPA (Layer protection analysis),
- odločitveno drevo (Decision tree),
- analiza človeške zanesljivosti (Human reliability analysis),
- analiza pentelj (Bow tie analysis),
- zanesljivo usmerjeno vzdrževanje RCM (Reliability centred maintenance),
- analiza napak v zasnovi (Sneak circuit analysis),
- Markova analiza (Markov analysis),
- Monte Carlo simulacija (Monte Carlo simulation),
- Bayesove statistike in mreže (Bayesian statistics and Bayes Nets),
- FN krivulje (FN curves),
- pokazatelji tveganj (Risk indices),
- matrika posledic in verjetnosti (Consequence/probability matrix),
- analiza stroškov in koristi (Cost/benefit analysis),
- analiza odločitev s pomočjo več meril MCDA (Multi-criteria decision analysis). [2]

Za potrebe enotnega ocenjevanja tveganj v različnih sistemih organizacij sem zaradi enostavnosti uporabil matriko posledic in verjetnosti (Consequence/probability matrix), seveda pa se organizacije lahko odločajo tudi za drugačne tehnike ocenjevanja tveganj. Prednosti, ki jih ima omenjena tehnika, so predvsem enostavnost uporabe, hitra razvrstitev tveganj, transparentnost pri ocenjevanju stroškov in koristi ter nabor natančnih podatkov pred odločitvijo o posameznem tveganju [2]. Zaradi tega je uporaba v organizacijah, ki so na začetku poti ocenjevanja tveganj ali pa se z ocenjevanjem tveganj do sedaj niso ukvarjale, smiselna in priporočljiva - način je opisan pri ocenjevanju tveganj pri posameznih sistemih vodenja.

1.4 Dobre prakse uporabe ocene tveganja - sistemi vodenja (ISO standardi)

Sistem vodenja je struktura procesov in postopkov, ki zagotavlja, da lahko organizacija izpolni vse naloge, potrebne za dosego svojih ciljev. [4]

Večja in kompleksnejša je organizacija, bolj je potrebno beležiti delovne procese. Ta proces sistematiziranja postopkov je znan kot sistem vodenja. [5]

ISO standardi sistemov vodenja določajo model, ki se lahko uporabi za vzpostavitev in izvajanje sistemov vodenja. Ti standardi so uporabni za vse organizacije, ne glede na to, kakšen izdelek ali storitev organizacije ponujajo.

Prednosti učinkovitega sistema za upravljanje vključujejo:

- učinkovitejšo rabo virov,
- izboljšano upravljanje s tveganji,
- povečano zadovoljstvo odjemalcev. [5]

Vsak posamezen standard sistema vodenja predstavlja en del vodenja organizacije, zato je povsem razumljivo, da njihovo združevanje daje možnost za izboljšavo celotnega sistema vodenja organizacije.

Osnovni standard sistema vodenja organizacije je trenutno standard za sistem vodenja kakovosti ISO 9001. Ta je tudi osnova ostalim standardom, ki se nanj nadgrajujejo in ga razširjajo. Katerega od obstoječih standardov bo organizacija poleg standarda ISO 9001 še uporabljala, pa je odvisno od dejavnosti posamezne organizacije.

Organizacija, ki s svojo dejavnostjo pomembno vpliva na okolje, bo uvedla sistem, ki je usklajen s standardom ISO 14001. Organizacija, ki upravlja s podatki, bo uporabila enega od informacijskih standardov (ISO/IEC 27001, ISO/IEC 20000-1). Organizacija, ki je udeležena v prehranski verigi, bo uvedla sistem HACCP ali standard ISO 22000. Organizacija, ki se ukvarja z varstvom pri delu in varovanjem zdravja, bo uporabljala standard BS OHSAS 18001.

Organizacija s področja avtomobilske industrije, bo uporabila ustrezen standard za avtomobilsko industrijo ISO/TS 16949, organizacija, ki izdeluje medicinske izdelke, pa npr. standard ISO 13485. Posamezna organizacija lahko svoj sistem vodenja kakovosti nadgradi tudi z več dodatnimi sistemi, odvisno od njene dejavnosti. [3]

S sistemi vodenja se srečuje večina organizacij, ki želijo dolgoročno poslovati ter dokazovati uspešnost vodenja pred odjemalci in dobavitelji. S tem pa morajo te organizacije poskrbeti tudi za ustrezno upravljanje s tveganji.

1.5 Ocenjevanje tveganj v sistemih vodenja

Ocenjevanje tveganj v sistemih vodenja ni nekaj novega. Pojavljati se je začelo predvsem s standardom ISO/IEC 27001:2005, ker je bila ocena tveganja ključni element vzpostavitve sistema vodenja. Sedaj se pojavlja še v drugih standardih sistemov vodenja, kot so ISO 9001, ISO 14001, ISO 45001 in je osnovni mehanizem, preko katerega naj bi organizacije ocenjevale tveganja poslovnih procesih ter gradile uspešno poslovanje.

To se je zgodilo s poenotenjem standardov in vzpostavitvijo mehanizma ocenjevanja tveganj kot osnovnega mehanizma sistemov vodenja. Ocena tveganja v organizaciji je sedaj ključni mehanizem, ki pomaga poslovodstvu organizacije, da se na podlagi ocene tveganj lahko odloča o poslovanju organizacije, vse od strateškega planiranja do upravljanja z viri.

1.5.1 Viri, ki so predmet ocene tveganja

Osnovna predpostavka pri ocenjevanju tveganj, ki jo podajam, je, da se samo ocenjevanje tveganj lahko izvaja nad izbranim obsegom - poslovnimi procesi, organizacijskimi enotami oziroma viri. Vendar pa se moramo zavedati, da sta tudi poslovni proces oziroma organizacijska enota sestavljena iz posameznih virov organizacije. Zato je smiselno pri ocenjevanju tveganj najprej definirati vire, na katerih se bo ocenjevanje tveganj izvajalo. Pri tem se moramo zavedati, da viri spadajo v posamezne poslovne procese ali/in organizacijske enote, tako da se ocenjevanje tveganj nad poslovnimi procesi ali organizacijskimi enotami izvaja glede na vse vključene vire v posamezen poslovni proces ali organizacijsko enoto.

1.5.2 Grožnje, ki so predmet ocene tveganja

Grožnje, ki pretijo posamezni organizaciji, se zaradi okolja in značilnosti poslovanja razlikujejo od groženj, ki pretijo drugim organizacijam. Posamezna organizacija mora smiselno definirati grožnje, ki se lahko zgodijo v njenem poslovanju, seveda s stališča dejavnosti posamezne organizacije in zakonodaje ter standardov, ki jih mora organizacija upoštevati. Za ustrezno in celovito ocenjevanje tveganj je smiselno, da organizacija pripravi katalog groženj, ki jo zadevajo, kar je razvidno iz okolja organizacije in virov, nad katerimi se bo izvajala ocena tveganja. V kolikor gledamo sistem vodenja kakovosti, so ti viri izdelki in storitve, v primeru sistema ravnanja z okoljem so to viri, povezani z okoljskimi vidiki, v primeru varstva in zdravja pri delu so to zaposleni, v primeru informacijske varnosti so to podatki. V obseg ocenjevanja tveganj je potrebno vključiti vse grožnje, ki so povezane z viri in posledično organizacijskimi enotami ali poslovnimi procesi, ki smo jih definirali v obsegu.

1.5.3 Ranljivosti, ki so predmet ocene tveganja

Ranljivosti so prav tako kot grožnje odvisne od virov in se z grožnjami neposredno povezujejo. Tako lahko na podlagi ranljivosti posameznega vira definiramo, katere grožnje iz kataloga groženj so relevantne pri samem ocenjevanju tveganj in na kakšen način se lahko izkazujejo. Pri tem moramo upoštevati, da verjetnost uresničitve grožnje za razliko od posledic uresničitve ocenjujemo tako na podlagi kataloga groženj kot tudi ranljivosti, saj verjetnost uresničitve grožnje dejansko pomeni že vključevanje ranljivosti posameznega vira pri izbiri stopnje verjetnosti uresničitve grožnje. Če se npr. incident lahko zgodi 1x mesečno, to pomeni, da je prisotna grožnja, ravno tako pa je ta vir tudi zelo ranljiv, drugače do incidenta ne bi moglo prihajati tako pogosto.

1.5.4 Ocena tveganja

Tveganje se lahko izračunava kot izračun verjetnosti in posledic uresničitve grožnje v dvodimenzionalni matriki. Ker sem za potrebe enotnega ocenjevanja tveganj v različnih sistemih organizacij zaradi enostavnosti uporabil matriko posledic in verjetnosti (Consequence/probability matrix), se ocenjevanje tveganj izvaja na način, kot ga opredeljuje Slika 2:

			Posledice					
			Incident ne povzroči škode organizaciji, ne zaustavi delovanja organizacije, ne povzroči izgube ali zlorabe podatkov, ni nevarnosti za zdravje in življenje zaposlenih.	Incident povzroči škodo v posamezni organizacijski enoti, izpad delovanja organizacije je še sprejemljiv, lahko pride do izgube podatkov, možne so lažje poškodbe zaposlenih.	Incident povzroči škodo v več organizacijskih enotah, izpad delovanja organizacije je še sprejemljiv, lahko pride do izgube ali zlorabe podatkov, verjetne so poškodbe zaposlenih.	Incident povzroči večjo škodo za organizacijo, izpad delovanja organizacije za daljši čas, velika je možnost izgube ali zlorabe podatkov, možne so večje poškodbe zaposlenih.	Incident povzroči veliko škodo organizaciji, preživetje organizacije je oteženo, delovanje organizacije ni možno za daljši čas, možna je izguba ali zloraba večine podatkov, verjetne so težje poškodbe zaposlenih.	Incident lahko povzroči konec poslovanja organizacije, izpad delovanja za daljši čas, izgubo ali zlorabo vseh podatkov, možna je smrt ali težke poškodbe zaposlenih.
			1	2	3	4	5	6
Verjetnost	Incident se lahko zgodi večkrat mesečno.	E	4	3	2	1	1	1
	Incident se lahko zgodi 1x mesečno.	D	4	3	3	2	1	1
	Incident se lahko zgodi večkrat letno.	C	5	4	3	2	2	1
	Incident se zgodi 1x letno ali manj pogosto.	B	5	4	3	3	2	1
	Incident se zgodi 1x na desetletje ali manj pogosto.	A	5	5	4	3	2	2

Slika 2: Matrika ocenjevanja tveganja v programski opremi OTO

Organizacija ob tem določi vire, ki so v obsegu ocene tveganja, določi značilnosti in vrednosti virov ter na podlagi značilnosti virov določi ranljivosti le-teh. Prav tako, kot se določi značilnosti in vrednosti posameznih virov, se lahko oceni značilnost in vrednost organizacijskih enot in poslovnih procesov, kar pomaga pri analizi stroškov in koristi – podlagi za poslovno odločanje.

Nato se vzpostavi katalog groženj, s pomočjo katerega se lahko začne z ocenjevanjem tveganja ter določi, kaj pomeni za organizacijo posledica uresničitve posamezne grožnje (kvalitativna in kvantitativna merila).

Na podlagi izkušenj poslovanja in vodenja organizacije se določi nivoje verjetnosti uresničitve posameznih groženj in s posameznimi vodji organizacijskih enot ali skrbniki procesov izvede ocenjevanje tveganj. Pri tem se lahko enostavno izračuna tudi škoda, ki bi nastala ob uresničitvi grožnje, če vemo, kakšna je vrednost posameznih sredstev, organizacijskih enot oziroma poslovnih procesov.

1.5.5 Zakonodaja in zahteve standardov, pravilnikov

Zakonodaje, ki bi opredeljevala zahteve za ocenjevanje tveganj, je veliko, vendar je malokrat v samih zakonodajnih določilih natančno določeno, kakšno tehniko ocenjevanja tveganj (metodologijo) naj uporablja organizacija. To je deloma razumljivo, saj se organizacije razlikujejo med seboj in bi preveč uniformirana tehnika ocenjevanja tveganj (metodologija) lahko pomenila težave pri izvajanju ocene tveganja oziroma bi lahko privedla do napačnih rezultatov, zato se velikokrat zakonodajna določila navezujejo na dobre prakse ali standarde oziroma prepuščajo organizaciji proste roke pri ocenjevanju tveganj. Za primer dobre prakse lahko vzamemo standarde sistemov vodenja in njihove zahteve glede ocenjevanja tveganj ter smiselnost enotne ocene tveganja, ki lahko predstavlja tudi mehanizem združevanja sistemov vodenja v enoten in celovit sistem.

1.5.6 ISO 9001 in tveganja

Uporaba mednarodnega standarda za sisteme vodenja kakovosti ISO 9001 se je od svoje prve izdaje leta 1987 močno razširila po vsem svetu in tako je danes v uporabi v zasebnem sektorju, javni upravi in drugih organizacijah. Število uporabnikov še vedno narašča. Danes je certificiranih že več kot 1.1 milijona sistemov vodenja z zahtevami standarda ISO 9001 v organizacijah širom po svetu.

Standard ISO 9001 je bil že večkrat prenovljen, in sicer leta 1994, 2000, 2008 in 2015. Ob zadnji prenovi je bila spremenjena struktura standarda, ki sedaj velja za vse mednarodne standarde in je za vse sisteme vodenja enaka. Prenovljena so načela kakovosti, postavljene nove zahteve glede odnosa organizacije do zunanjega in notranjega okolja ter postavljene nove zahteve glede obvladovanja tveganj.

Trenutna prenova daje standardu novo strateško usmeritev. Upošteva, da je zahteve sistema potrebno prilagoditi trenutnim in bodočim poslovnim okoliščinam. Vse bolj pomembno je ustrezno upravljanje s tveganji in priložnostmi ob upoštevanju zahtev zunanjega in notranjega okolja. Sistem vodenja kakovosti je tako postal še ustreznejše orodje za realizacijo strateških odločitev in izpolnjevanje poslanstva organizacij. [3]

Ker je ocenjevanje tveganj v tem standardu opredeljeno kot zahteva, sam standard pa se povezuje glede ocenjevanja tveganj s standardom ISO 31000, lahko za ocenjevanje uporabimo matriko posledic in verjetnosti (Consequence/probability matrix), ki je opisana v Sliki 2. Vendar pa je potrebno ustrezno pripraviti tudi kataloge groženj, kjer pa se lahko naslonimo na poslovne zahteve organizacije in vključimo vse tiste grožnje, ki so vezane na poslovanje, notranje in zunanje okolje ter odnos do odjemalcev. Na ta način lahko pripravimo splošni katalog groženj, ki ga potem organizacija prilagodi svojim posebnostim in obsega vsa tista področja, kjer bi lahko prišlo do škodljivih dogodkov za poslovanje. Primer splošnega kataloga groženj je opredeljen v Sliki 3. Ta katalog groženj pa se potem lahko povezuje tudi z ostalimi sistemi vodenja, ki jih ima organizacija in kjer je potrebno ocenjevati tveganja.

Nabor groženj je podan, določeno je, na katere tipe virov lahko posamezna grožnja vpliva, tako da se ocenjuje posamezne grožnje samo na objektih (virih), za katere so relevantne (glej oznake na Sliki 3).

Predvidena verjetnost uresničitve groženj:			Nabor groženj ISO/IEC 9001	Vpliv na tip vira										
				Zaposleni	Prostori	Podporna infrastruktura	Delovna oprema	Računalniška strojna oprema	Računalniške aplikacije	Komunikacije	Papirna dokumentacija	Elektronska dokumentacija in podatki	Storitve in programska oprema	Zunanji sodelavci
Okoljske nesreče														
Incident se zgodi 1x na desetletje ali manj pogosto.	A	1	Večje elementarne nesreče (potresi, plazovi, poplave, izredni vremenski dogodki).	x	x	x	x	x		x	x	x	x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	2	Ogenj (požari v objektu, okolici ali na napeljavah, požigi).	x	x	x	x	x		x	x	x	x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	3	Zalitje vode (izlivi iz vodovodne napeljave, meteorne vode, puščanje streh).		x	x	x	x			x		x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	4	Industrijske nesreče (onesnaženje, eksplozije, razlitje nevarnih snovi).	x	x	x	x	x			x	x	x	
Izpadi podpornih storitev														
Incident se zgodi 1x letno ali manj pogosto.	B	5	Izpad oskrbe z električno energijo.			x	x	x	x	x		x	x	x
Incident se lahko zgodi večkrat letno.	C	6	Izpad komunikacijskih storitev.					x	x	x		x	x	x
Incident se zgodi 1x letno ali manj pogosto.	B	7	Neustrezno izvajanje storitev zunanjih ponudnikov (dobavitelji storitev).		x	x	x	x	x	x	x	x	x	x
Incident se lahko zgodi večkrat letno.	C	8	Izpad podpornih sistemov za proizvodnjo ali delovanje organizacije (servisne storitve).		x	x	x	x	x	x		x	x	x
Delovne nesreče in izpadi opreme														
Incident se zgodi 1x letno ali manj pogosto.	B	9	Nenapovedana odsotnost zaposlenih (smrt, bolezen, nesreča).	x									x	x
Incident se lahko zgodi večkrat letno.	C	10	Okvara/izpad delovne opreme (stroji, linije, računalniška oprema).				x	x	x	x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	11	Odpoved delovne opreme za prevzem proizvodov ali storitev dobaviteljev (nedelovanje logistike, izpad skladiščenja).				x	x	x	x	x	x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	12	Odpoved opreme za posredovanje proizvodov ali storitev odjemalcem (nedelovanje logistike, izpad trgovine).				x	x	x	x	x	x	x	
Incident se lahko zgodi večkrat letno.	C	13	Izpad delovne opreme za nadzor nad proizvodi in storitvami (nepopolne evidence, nezmožnost				x	x	x	x	x	x	x	

			sledenja izdelku, izpad računalniške podpore, neizvajanje inventure).											
Izpadi razvoja in priprave proizvodov in storitev														
Incident se zgodi 1x na desetletje ali manj pogosto.	A	14	Razvoj in priprava proizvodov in novih storitev se ne izvaja zaradi zasedenosti kadra s proizvodnjo ali izvedbe storitev.	x									x	x
Incident se lahko zgodi večkrat letno.	C	15	Predolgi časi razvoja in priprave na proizvodnjo ali nove storitve.	x									x	x
Incident se zgodi 1x letno ali manj pogosto.	B	16	Neustrezno znanje zaposlenih za razvoj ali pripravo proizvodov in storitev.	x									x	x
Incident se zgodi 1x letno ali manj pogosto.	B	17	Preveliki stroški razvoja ali priprave novih storitev.	x									x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	18	Izguba zaupnosti papirne in elektronske dokumentacije za razvoj ali pripravo novih storitev (industrijsko vohunstvo).								x	x		
Incident se lahko zgodi večkrat letno.	C	19	Slabšanje papirne in elektronske dokumentacije (izguba, uničenje, poškodovanje zaradi neustrezne hrambe).								x	x		
Izpadi proizvodnje ali izvedbe storitev														
Incident se zgodi 1x letno ali manj pogosto.	B	20	Izpad dobave materialov ali vhodnih storitev za proizvodnjo ali izvedbo storitev.									x	x	x
Incident se lahko zgodi večkrat letno.	C	21	Neustrezna kakovost materialov ali vhodnih storitev za proizvodnjo ali izvedbo storitev.										x	x
Incident se zgodi 1x letno ali manj pogosto.	B	22	Neustrezno izvajanje procesov proizvodnje ali izvedbe storitev (niso določene odgovorne osebe, roki izvedbe, cilji).	x							x	x	x	x
Incident se zgodi 1x letno ali manj pogosto.	B	23	Premajhna zmogljivost (premalo delovne opreme, prostorov, zaposlenih) za doseganje ustreznega nivoja proizvodnje ali izvedbe storitev.	x	x	x	x	x	x	x	x	x	x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	24	Zaustavitev proizvodnje zaradi neskladnosti z zahtevami zakonodajnih ali nadzornih organov.	x	x	x	x						x	
Incident se zgodi 1x na desetletje ali manj pogosto.	A	25	Stavka, izredna stanja, zaustavitev proizvodnje ali izvedbe storitev zaradi zunanjih dogodkov.	x									x	x
Incident se zgodi 1x letno ali manj pogosto.	B	26	Izguba ključnih zaposlenih zaradi neustreznih delovnih pogojev (plačilo, neprimeren karierni razvoj).	x										
Incident se zgodi 1x letno ali manj pogosto.	B	27	Neustrezno delovanje poslovnega informacijskega sistema (kontakt z odjemalci).					x	x	x		x		
Incident se zgodi 1x letno ali manj pogosto.	B	28	Neustrezno delovanje industrijskih informacijskih sistemov (SCADA) ali namenske računalniške opreme (izvedba proizvodnje ali storitev).					x	x	x		x	x	
Izpadi prodaje in nezadovoljstvo odjemalcev														

Incident se zgodi 1x letno ali manj pogosto.	B	29	Neustrezna ponudba proizvodov in storitev (oglaševanje, predprodajni postopki).	x									x	x
Incident se lahko zgodi večkrat letno.	C	30	Neustrezna kakovost proizvoda ali storitve.										x	
Incident se lahko zgodi večkrat letno.	C	31	Nezadovoljstvo odjemalcev s prodajnim procesom.	x									x	x
Incident se zgodi 1x letno ali manj pogosto.	B	32	Nezadovoljstvo odjemalcev z garancijskimi postopki ali servisom.	x									x	x
Incident se zgodi 1x letno ali manj pogosto.	B	33	Neustrezni reklamacijski postopki.	x									x	x
Incident se lahko zgodi večkrat letno.	C	34	Vračila zaradi neskladnosti proizvoda ali storitve z navedenimi specifikacijami ali opisom.										x	
Incident se lahko zgodi večkrat letno.	C	35	Popravki ali ponovna proizvodnja oziroma izvedba storitev zaradi napak na proizvodu ali storitvi.										x	
Incident se lahko zgodi večkrat mesečno.	E	36	Neustrezni sistem kakovosti - pomanjkanje sodelovanja med organizacijskimi enotami oziroma v procesih (razvoj, proizvodnja, zagotavljanje storitev, prodaja).	x									x	x
Incident se lahko zgodi večkrat letno.	C	37	Neustrezno delovanje poslovnega informacijskega sistema (obračun, blagajna).			x		x	x	x		x	x	x
Incident se lahko zgodi večkrat letno.	C	38	Neustrezno delovanje spletnih strani za prodajo proizvodov in storitev.					x	x	x		x	x	x
Incident se lahko zgodi 1x mesečno.	D	39	Neustrezno komuniciranje s strankami glede proizvodov in storitev po prodaji.	x			x	x	x	x		x	x	
Incident se zgodi 1x na desetletje ali manj pogosto.	A	40	Izguba posameznih ključnih odjemalcev proizvodov in storitev (nad 25 % obsega poslovanja).										x	

Slika 3: Katalog groženj metodologije ISO 9001 (poslovanje organizacij)

1.5.6.1 Metodologija upravljanja tveganj ISO/IEC 9001

Metodologija opredeljuje, da so vsa tveganja nivoja 4 ali 5 nesprejemljiva in se mora zanju sprejeti ustrezne ukrepe. Upravljanje s tveganji je skladno s standardom ISO 31000, kar pomeni, da se za vsako nesprejemljivo tveganje odloči, na kakšen način se ga bo reševalo:

- spreminjanje tveganja – uvedba, odstranjevanje, spreminjanje kontrol varovanja,
- zadrževanje tveganja – neizvajanje ukrepov za zmanjševanje tveganj,
- izogibanje tveganja – umik aktivnosti,
- porazdelitev tveganja – deljenje z ostalimi deležniki tveganj.

1.5.6.2 ISO 14001 in tveganja

V letu 2015 je bil prav tako izdan standard ISO 14001 (Sistemi ravnanja z okoljem – Zahteve z navodili za uporabo). Od njegove prve izdaje v letu 1996 se je skladno z zahtevami standarda certificiralo več kot 250.000 organizacij v 155 državah širom po svetu. [3]

V novem standardu se prepoznavanje in vrednotenje okoljskih vidikov in vplivov še vedno osredotoča na dejavnost ter proizvode in storitve, povezane z delovanjem organizacije. Veliko organizacij, ki so se uskladile s standardom, pa že uporablja tehnike ocenjevanja tveganj, ki podpirajo njihov pristop k okoljskim vidikom. Standard prinaša s sabo zahteve po uveljavljanju širšega modela obvladovanja tveganj, kar pomeni, da je potrebno oceno tveganja še bolj povezati s strateškimi cilji. Pri tem se je treba zavedati, da tveganja niso izključno povezana samo z okoljskimi vidiki, pač pa tudi s pravnimi in drugimi zahtevami o skladnosti poslovanja organizacije. [6]

1.5.6.3 ISO 45001 in tveganja

Dvajset let po objavi standarda BS 8800, prvega širše znanega standarda, ki je obravnaval sisteme vodenja varnosti in zdravja pri delu, namerava Mednarodna organizacija za standardizacijo prvič izdati mednarodni standard za to področje. To bo ISO 45001, ki bo obravnaval sistem vodenja varnosti in zdravja pri delu. Napisan bo v skladu z vodilom ISO o enotni strukturi standardov za sisteme vodenja, v veliki meri pa bo utemeljen na podlagi standarda BS OHSAS 18001. Če je pri sistemih vodenja kakovosti ocenjevanje tveganj na prvi pogled nova zahteva, je to pri sistemu vodenja varnosti in zdravja pri delu nekaj že znanega, vendar kljub temu ne brez možnosti za izboljšave. Z enako strukturo standardov za sisteme vodenja bo lažja tudi njihova sočasna uporaba in integracija. Pri uporabi in integraciji različnih vidikov vodenja (ISO 9001, ISO 14001) v enoten sistem vodenja organizacije bo vidik varnosti in zdravja lažje doprinesel k realizaciji strateških odločitev in izpolnjevanju poslanstva organizacij. [3]

1.5.7 ISO/IEC 27001 in tveganja

Standard ISO/IEC 27001 postavlja ocenjevanje tveganj na ključno mesto pri vzpostavitvi sistema vodenja. Področje ocenjevanja tveganj je natančno opredeljeno s standardom ISO/IEC 27005, kjer je natančno opredeljena tudi matrika posledic in verjetnosti (Consequence/probability matrix) ter primeri katalogov groženj, ranljivosti in virov.

Standard je postavil zahteve sistemov vodenja po poglavjih, ki jim sledijo tudi drugi sistemi vodenja v prenovljenih standardih. Najbolj je to razvidno pri uporabi mehanizma ocene tveganja. Ta je organizacijam omogočil, da se začnejo sistematično ukvarjati z zmanjševanjem tistih tveganj, ki lahko povzročijo težave pri samem poslovanju. S tem so se sistemi vodenja še bolj približali samemu poslovanju organizacij in omogočili, da se poslovanje izboljšuje tudi z vidika upravljanja poslovnih procesov, ocenjevanja vseh poslovnih in organizacijskih tveganj in ustreznega varovanja vseh virov organizacije.

Ocenjevanje tveganj poteka z ocenitvijo posledic in verjetnosti uresničitve groženj, pri čemer se verjetnost uresničitve predvideva iz vnaprej pripravljenih katalogov groženj. (Primer kataloga groženj za informacijsko varnost je naveden na Sliki 4.)

Nabor groženj je podan, določeno je, na katere tipe virov lahko posamezna grožnja vpliva, tako da se ocenjuje posamezne grožnje samo na objektih (virih), na katere lahko vplivajo (glej oznake na Sliki 4).

Predvidena verjetnost uresničitve groženj:			Nabor groženj ISO/IEC 27001	Vpliv na tip vira										
				Zaposleni	Prostori	Podporna infrastruktura	Delovna oprema	Računalniška strojna oprema	Računalniške aplikacije	Komunikacije	Papirna dokumentacija	Elektronska dokumentacija in podatki	Storitve in programska oprema	Zunanji sodelavci
Okoljske nesreče														
Incident se zgodi 1x na desetletje ali manj pogosto.	A	1	Večje elementarne nesreče (potresi, plazovi, poplave, izredni vremenski dogodki).	x	x	x	x	x		x	x	x	x	x

Incident se zgodi 1x na desetletje ali manj pogosto.	A	2	Ogenj (požari v objektu, okolici ali na napeljavah, požigi).	x	x	x	x	x		x	x	x	x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	3	Zalitje vode (izlivi iz vodovodne napeljave, meteorne vode, puščanje streh).		x	x	x	x			x		x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	4	Industrijske nesreče (onesnaženje, eksplozije, razlitje nevarnih snovi).	x	x	x	x	x			x	x	x	
Izpadi podpornih storitev														
Incident se zgodi 1x letno ali manj pogosto.	B	5	Izpad oskrbe z električno energijo.			x	x	x	x	x		x	x	
Incident se lahko zgodi večkrat letno.	C	6	Nihanja električne napetosti.										x	
Incident se lahko zgodi večkrat letno.	C	7	Izpad komunikacijskih storitev.					x	x	x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	8	Neustrezno izvajanje storitev zunanjih ponudnikov (oblak, gostovanje).						x	x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	9	Izpad klimatskega sistema.			x		x					x	
Delovne nesreče in izpadi opreme														
Incident se zgodi 1x letno ali manj pogosto.	B	10	Nenapovedana odsotnost zaposlenih (smrt, bolezen, nesreča).	x									x	x
Incident se lahko zgodi večkrat letno.	C	11	Okvara/izpad uporabniške računalniške in/ali mobilne opreme.					x	x			x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	12	Okvara/izpad strežniške računalniške opreme.					x	x			x	x	
Incident se lahko zgodi večkrat letno.	C	13	Okvara/izpad komunikacijske opreme.						x	x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	14	Izpad/nepravilno delovanje programske opreme.						x			x	x	
Zloraba podatkov														
Incident se zgodi 1x na desetletje ali manj pogosto.	A	15	Slabšanje papirne dokumentacije (uničenje, poškodovanje zaradi neustrezne hrambe).								x		x	
Incident se zgodi 1x letno ali manj pogosto.	B	16	Kraja/izguba računalniške in mobilne opreme.					x	x			x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	17	Kraja/namerno uničenje podatkov in dokumentov.								x	x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	18	Nepooblaščen dostop do podatkov in dokumentov.								x	x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	19	Nepooblaščeno razkrivanje podatkov in dokumentov.								x	x	x	
Incident se lahko zgodi 1x mesečno.	D	20	Izguba/nenamerno uničenje podatkov in dokumentov.								x	x	x	
Zloraba informacijskega sistema														
Incident se zgodi 1x letno ali manj pogosto.	B	21	Zloraba administratorskih pravic dostopa do računalniškega sistema.						x	x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	22	Zloraba uporabniških pravic dostopa do računalniškega sistema.						x	x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	23	Socialni inženiring.	x									x	x

Incident se lahko zgodi večkrat mesečno.	E	24	Zlonamerna programska oprema (virusi, črvi, trojanski konji, škodljiva koda).					x	x			x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	25	Vdori/napadi v informacijski sistem.					x	x			x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	26	Preusmerjanje internetnega prometa (lastna omrežja, preusmeritev elektronske pošte).							x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	27	Prestrezanje podatkov in dokumentov v računalniškem sistemu ali omrežju.						x	x		x	x	
Incident se zgodi 1x letno ali manj pogosto.	B	28	Kraja identitete (izkazovanje lažne identitete).	x	x	x	x	x	x	x	x	x	x	x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	29	Poneverba spletne strani.						x			x	x	
Neustrezno upravljanje informacijskega sistema														
Incident se lahko zgodi večkrat letno.	C	30	Neizvajanje varnostne politike.	x									x	x
Incident se lahko zgodi 1x mesečno.	D	31	Posojanje gesel ali uporaba skupinskih gesel.	x										x
Incident se lahko zgodi večkrat letno.	C	32	Uporaba nedovoljene programske opreme.	x					x			x		x
Incident se zgodi 1x na desetletje ali manj pogosto.	A	33	Napake pri vzdrževanju informacijskega sistema.	x					x			x		x
Incident se lahko zgodi 1x mesečno.	D	34	Neposodabljanje programske opreme.						x			x		
Incident se lahko zgodi 1x mesečno.	D	35	Pomanjkljive revizijske sledi.						x			x		
Incident se lahko zgodi večkrat letno.	C	36	Neizvajanje/nepravilno izvajanje varnostnega kopiranja.						x			x		
Incident se lahko zgodi 1x mesečno.	D	37	Nenadzorovana uporaba lastne računalniške opreme.	x					x			x		x
Incident se lahko zgodi večkrat letno.	C	38	Nepooblaščeno priključevanje v omrežje (brezžično ali žično).	x						x		x	x	x
Incident se lahko zgodi večkrat mesečno.	E	39	Neustrezno upravljanje mobilnih naprav.					x						
Incident se zgodi 1x letno ali manj pogosto.	B	40	Neprimerna povezava industrijskih informacijskih sistemov in klasičnih informacijskih sistemov.				x	x	x	x		x	x	

Slika 4: Katalog groženj metodologije ISO/IEC 27001 (varovanje podatkov)

1.5.7.1 Metodologija upravljanja tveganj ISO/IEC 27001

Metodologija opredeljuje, da so vsa tveganja, nivoja 4 ali 5 nesprejemljiva in se mora za njiju sprejeti ustrezne ukrepe. Upravljanje s tveganji je skladno s standardom ISO/IEC 27005:2011, kar pomeni, da se za vsako nesprejemljivo tveganje odloči, na kakšen način se ga bo reševalo:

- spreminjanje tveganja – uvedba, odstranjevanje, spreminjanje kontrol varovanja,
- zadrževanje tveganja – neizvajanje ukrepov za zmanjševanje tveganj,
- izogibanje tveganja – umik aktivnosti,
- porazdelitev tveganja – deljenje z ostalimi deležniki tveganj.

Za razliko od ISO 9001, ISO 14001 in ISO 45001 se pri tej metodologiji ukrepi, odgovorne osebe in roke izvedbe (enkratno ali ponavljajoče izvajanje), ki se določijo, poveže s kontrolami iz dodatka A standarda ISO/IEC 27001:

A.5.1.1.	Politike za varovanje informacij	Določiti se mora sklop politik za varovanje informacij, ki jih odobri vodstvo, ter jih objavi ti in sporočiti zaposlenim in ustreznim zunanjim strankam.
A.5.1.2.	Pregled politik za varovanje informacij	Politike za varovanje informacij se morajo pregledovati v načrtovanih intervalih oz., če se pojavijo pomembne spremembe, da se zagotovijo njihova nenehna ustreznost, zadostnost in uspešnost.
A.6.1.1.	Vloge in odgovornosti na področju varovanja informacij	Določiti in dodeliti se morajo vse odgovornosti na področju varovanja informacij.
A.6.1.2.	Razmejitev dolžnosti	Nasprotujoče si naloge in področja odgovornosti se morajo razmejiti, da se zmanjšajo možnosti za nepooblaščeno ali nenamerno spreminjanje ali zlorabo sredstev organizacije.
A.6.1.3.	Stiki s pristojnimi organi	Vzdrževati se morajo ustrezni stiki s pristojnimi organi.
A.6.1.4.	Stik s specifičnimi interesnimi skupinami	Vzdrževati se morajo ustrezni stiki s specifičnimi interesnimi skupinami ali z drugimi strokovnimi forumi in združenji za varovanje.
A.6.1.5.	Varovanje informacij v upravljanju projektov	Varovanje informacij se mora obravnavati v okviru upravljanja projektov ne glede na vrsto projekta.
A.6.2.1.	Politika na področju mobilnih naprav	Sprejeti se morajo politika in podporni varnostni ukrepi za upravljanje tveganj, nastalih z uporabo mobilnih naprav.
A.6.2.2.	Delo na daljavo	Izvajati se morajo politika in podporni varnostni ukrepi za zaščito informacij, do katerih se dostopa, se obdelujejo ali se hranijo na mestih dela na daljavo.
A.7.1.1.	Preverjanje	Varnostna preverjanja vseh kandidatov za zaposlitev se morajo izvajati v skladu z ustreznimi zakoni, predpisi in etiko ter sorazmerno s poslovnimi zahtevami, razvrstitvijo informacij, do katerih bodo dostopali, ter zaznanimi tveganji.
A.7.1.2.	Določila in pogoji za zaposlitev	Pogodbeni dogovori z zaposlenimi in pogodbeniki morajo vsebovati njihove odgovornosti in odgovornosti organizacije za varovanje informacij.
A.7.2.1.	Odgovornosti vodstva	Vodstvo mora od zaposlenih in pogodbenikov zahtevati varnostno ravnanje v skladu z vzpostavljenimi politikami in postopki organizacije za varovanje informacij.
A.7.2.2.	Ozaveščenost, izobraževanje in usposabljanje o varovanju informacij	Vsi zaposleni v organizaciji in po potrebi tudi pogodbeniki morajo biti ustrezno ozaveščeni ter seznanjeni z rednimi posodobitvami politik in postopkov varovanja informacij v organizaciji, pomembnih za njihovo delovno mesto.
A.7.2.3.	Disciplinski postopek	Obstajati mora formalni in sporočeni disciplinski postopek za ukrepanje proti zaposlenim, ki so kršili varovanje informacij.
A.7.3.1.	Prekinitev ali sprememba zaposlitvenih odgovornosti	Odgovornosti in dolžnosti na področju varovanja informacij, ki ostanejo veljavne po prekinitvi ali spremembi zaposlitve, se morajo določiti, sporočiti zaposlenemu ali pogodbeniku ter izvrševati.
A.8.1.1.	Popis sredstev	Viri, povezani z informacijami in napravami za obdelavo informacij, se morajo prepoznati ter pripraviti in vzdrževati se mora popis teh sredstev.
A.8.1.2.	Lastništvo nad viri	Viri, vzdrževani v okviru popisa, morajo biti v lastništvu.
A.8.1.3.	Sprejemljiva uporaba virov	Pravila za sprejemljivo uporabo virov, povezanih z informacijami in napravami za obdelavo informacij, se morajo prepoznati, dokumentirati in izvajati.
A.8.1.4.	Vračilo sredstev	Vsi zaposleni in uporabniki zunanje stranke morajo po prenehanju zaposlitve, pogodbe ali dogovora vrniti vse vire organizacije, ki jih posedujejo.
A.8.2.1.	Razvrstitev informacij	Informacije se morajo razvrščati glede na zakonske zahteve, vrednost, kritičnost in občutljivost na nepooblaščeno razkritje ali spreminjanje.
A.8.2.2.	Označevanje informacij	Razviti in izvajati se mora ustrezen niz postopkov za označevanje informacij v skladu z informacijsko razvrstitveno shemo, ki jo je sprejela organizacija.
A.8.2.3.	Ravnanje z informacijami in informacijskimi viri	Razviti in izvajati se morajo postopki za ravnanje z informacijami in informacijskimi viri v skladu z informacijsko razvrstitveno shemo, ki jo je sprejela organizacija.
A.8.3.1.	Upravljanje izmenljivih nosilcev podatkov/informacij	Izvajati se morajo postopki za ravnanje z odstranljivimi nosilci podatkov/informacij v skladu z razvrstitveno shemo, ki jo je sprejela organizacija.
A.8.3.2.	Odstranjevanje nosilcev podatkov/informacij	Ko nosilci niso več potrebni, se morajo varno odstraniti z uporabo formalnih postopkov.

A.8.3.3.	Prenos fizičnih nosilcev podatkov/informacij	Nosilci podatkov/informacij, ki vsebujejo informacije, se morajo zaščititi pred nepooblaščenim dostopom, zlorabo ali okvaro med prenašanjem.
A.9.1.1.	Politika nadzora dostopa	Vzpostaviti, dokumentirati in pregledovati se mora politika nadzora dostopa, ki temelji na poslovnih zahtevah in zahtevah informacijske varnosti.
A.9.1.2.	Dostop do omrežij in omrežnih storitev	Uporabniki morajo dobiti dostop le do omrežij in omrežnih storitev, za uporabo katerih so bili posebej pooblaščeni.
A.9.2.1.	Registracija in izbris registracije uporabnika	Izvesti se mora formalen postopek za registracijo in izbris registracije uporabnika, da se omogoči dodeljevanje pravic dostopa.
A.9.2.2.	Zagotavljanje dostopa uporabnikom	Izvesti se mora formalen proces zagotavljanja dostopa uporabnikom, da se pravice dostopa dodelijo ali prekličejo za vse vrste uporabnikov za vse sisteme in storitve.
A.9.2.3.	Upravljanje posebnih pravic dostopa	Dodelitev in uporaba posebnih pravic dostopa se morata omejiti in nadzorovati.
A.9.2.4.	Upravljanje zaupnih informacij uporabnikov za preverjanje verodostojnosti	Dodeljevanje zaupnih informacij za preverjanje verodostojnosti se mora nadzorovati prek formalnega procesa upravljanja.
A.9.2.5.	Pregled uporabniških pravic dostopa	Lastniki sredstev morajo pregledovati uporabniške pravice dostopa v rednih časovnih presledkih.
A.9.2.6.	Preklic ali prilagoditev pravic dostopa	Pravice dostopa vseh zaposlenih in zunanjih uporabnikov do informacij in naprav za obdelavo informacij se morajo odstraniti po prekinitvi njihove zaposlitve, pogodbe ali dogovora oziroma se prilagoditi spremembam.
A.9.3.1.	Uporaba zaupnih informacij za preverjanje verodostojnosti	Od uporabnikov se mora zahtevati, da sledijo praksam organizacije pri uporabi zaupnih informacij za preverjanje verodostojnosti.
A.9.4.1.	Omejitev dostopa do informacij	Dostop do informacij in sistemskih funkcij aplikacij se mora omejiti v skladu s politiko nadzora dostopa.
A.9.4.2.	Varni postopki prijave	Kadar tako zahteva politika nadzora dostopa, se mora dostop do sistemov in aplikacij nadzorovati z varnim prijavnim postopkom.
A.9.4.3.	Sistem upravljanja gesel	Sistemi za upravljanje gesel morajo biti interaktivni in morajo zagotavljati kakovostna gesla.
A.9.4.4.	Uporaba posebnih pomožnih programov	Uporaba pomožnih programov, ki bi lahko spremenili sistemske in aplikacijske kontrole, se mora omejiti in strogo nadzorovati.
A.9.4.5.	Nadzor dostopa do programske izvorne kode	Dostop do programske izvorne kode se mora omejiti.
A.10.1.1.	Politika uporabe kriptografskih kontrol	Za zaščito informacij se mora razviti in izvajati politika uporabe kriptografskih kontrol.
A.10.1.2.	Upravljanje ključev	Politika uporabe, zaščite in življenjske dobe kriptografskih ključev se mora razviti in izvajati v njihovem celotnem življenjskem ciklu.
A.11.1.1.	Varovanje fizičnih meja območja	Varovanje fizičnih meja območja z ovirami se mora določiti in uporabiti za zaščito območij, ki vsebujejo občutljive ali ključne informacije ter naprave za obdelavo informacij.
A.11.1.2.	Kontrole fizičnega pristopa	Varovana območja se morajo zaščititi z ustreznimi vhodnimi kontrolami, da se dovoljenje za dostop zagotovi samo pooblaščenim osebam.
A.11.1.3.	Varovanje pisarn, sob in naprav	Fizična varnost pisarn, sob in naprav se mora določiti in izvajati.
A.11.1.4.	Zaščita pred zunanjimi in okoljskimi grožnjami	Fizična zaščita pred poškodbami, naravnimi nesrečami, zlonamernimi napadi ali nesrečami se mora določiti in izvajati.
A.11.1.5.	Delo na varovanih območjih	Določiti in izvajati se morajo postopki za delo v varovanih območjih. .
A.11.1.6.	Dostavne in nakladalne površine	Dostopne točke, kot so območja za dostavo in nakladanje, ter druge točke, kjer nepooblaščene osebe lahko vstopajo v prostore, se morajo nadzorovati, in če je mogoče, izolirati od naprav za obdelavo informacij, da se prepreči nepooblaščen dostop.
A.11.2.1.	Namestitev in zaščita opreme	Oprema se mora namestiti in ščititi tako, da so tveganja zaradi okoljskih groženj in nevarnosti ter priložnosti za nepooblaščen dostop čim manjši.

A.11.2.2.	Podporna oskrba	Oprema se mora zaščititi pred odpovedmi napajanja in drugimi motnjami, ki jih povzročajo odpovedi v podporni oskrbi.
A.11.2.3.	Varnost ožičenja	Električno in telekomunikacijsko ožičenje, ki prenaša podatke ali podporne informacijske storitve, se morata zaščititi pred prestrezanjem, motnjami ali poškodbami.
A.11.2.4.	Vzdrževanje opreme	Oprema se mora pravilno vzdrževati, da se zagotovita njena razpoložljivost in celovitost.
A.11.2.5.	Odstranitev opreme	Oprema, informacije ali programska oprema se ne smejo odnašati iz prostorov brez predhodne odobritve.
A.11.2.6.	Varnost opreme zunaj prostorov organizacije	Varnost opreme zunaj organizacije se mora zagotoviti z upoštevanjem različnih tveganj pri delu zunaj prostorov organizacije.
A.11.2.7.	Varna odstranitev ali ponovna uporaba opreme	Preveriti se morajo vsi elementi opreme, ki vsebujejo medije za shranjevanje, ter zagotoviti, da so bili vsi občutljivi podatki in licenčna programska oprema odstranjeni ali varno prepisani pred odstranitvijo ali ponovno uporabo.
A.11.2.8.	Nenadzorovana uporabniška oprema	Uporabniki morajo zagotoviti, da je oprema brez nadzora ustrezno zaščitena.
A.11.2.9.	Politika čiste mize in praznega zaslona	Uvesti se morata politika čiste mize za papir in prenosne nosilce za shranjevanje ter politika praznega zaslona za naprave za obdelavo informacij.
A.12.1.1.	Dokumentirani postopki delovanja	Operativni postopki se morajo dokumentirati in dati na voljo vsem uporabnikom, ki jih potrebujejo.
A.12.1.2.	Upravljanje sprememb	Nadzorovati se morajo spremembe organizacije, poslovnih procesov, naprav za obdelavo informacij in sistemov, ki vplivajo na varovanje informacij.
A.12.1.3.	Upravljanje zmogljivosti	Uporaba virov se mora spremljati in prilagajati ter izvesti se morajo projekcije prihodnjih potreb po zmogljivosti za zagotovitev zahtevanega delovanja sistema.
A.12.1.4.	Ločevanje razvojnih, testnih in operativnih okolij	Razvojna, testna in operativna okolja se morajo ločiti, da so tveganja nepooblaščenega dostopa ali spremembe delujočega okolja manjši.
A.12.2.1.	Kontrole proti zlonamerni programski opremi	Za zaščito pred zlonamerno programsko opremo se morajo uvesti kontrole za zaznavanje, preprečevanje in obnovo ter ustrezni postopki ozaveščanja uporabnikov.
A.12.3.1.	Varnostno kopiranje informacij	Varnostne kopije podatkov, programske opreme in sistemskih nastavitev se morajo izdelovati in redno preskušati v skladu z dogovorjeno politiko varnostnega kopiranja.
A.12.4.1.	Beleženje dogodkov	Zapisovati, hraniti in redno pregledovati se morajo dnevniki dogodkov, ki beležijo aktivnosti uporabnikov, izjeme, okvare in dogodke varovanja informacij.
A.12.4.2.	Zaščita zabeleženih informacij	Naprave za beleženje in zabeležene informacije se morajo zaščititi pred nedovoljenimi posegi in nepooblaščenim dostopom.
A.12.4.3.	Beleženje aktivnosti administratorjev in operaterjev	Aktivnosti sistemskega administratorja in sistemskega operaterja se morajo beležiti, dnevniki pa se morajo zaščititi in redno pregledovati.
A.12.4.4.	Uskladitev ur	Ure vseh pomembnih sistemov za obdelavo informacij v organizaciji oziroma varnostni domeni se morajo uskladiti z enotnim referenčnim časovnim virom.
A.12.5.1.	Namestitev programske opreme na operativne sisteme	Izvajati se morajo postopki za nadzor namestitev programske opreme na operativne sisteme.
A.12.6.1.	Upravljanje tehničnih ranljivosti	Pravočasno se morajo pridobiti informacije o tehničnih ranljivostih informacijskih sistemov v uporabi, ovrednotiti izpostavljenost organizacije takim ranljivostim ter sprejeti ustrezni ukrepi za reševanje povezanega tveganja.
A.12.6.2.	Omejitve pri namestitvi programske opreme	Pravila, ki jih urejajo uporabniki za namestitev programske opreme, se morajo določiti in izvajati.
A.12.7.1.	Kontrole presoje / revizije informacijskih sistemov	Zahteve in aktivnosti presoj/revizij, ki vključujejo preverjanje operativnih sistemov, se morajo skrbno načrtovati ter o njih doseči soglasje, da se zmanjšajo motnje v poslovnih procesih.
A.13.1.1.	Omrežne kontrole	Omrežja se morajo ustrezno upravljati in nadzorovati, da se zaščitijo informacije v sistemih in aplikacijah.
A.13.1.2.	Varovanje omrežnih storitev	Prepoznati se morajo varnostni mehanizmi, ravni storitev in zahteve za upravljanje vseh omrežnih storitev ter vključiti v dogovore o omrežnih storitvah ne glede na to, ali so te storitve notranje ali jih zagotavljajo zunanji izvajalci.
A.13.1.3.	Ločevanje v omrežjih	Skupine informacijskih storitev, uporabnikov in informacijskih sistemov se morajo v omrežjih ločiti.

A.13.2.1.	Politike in postopki prenosa informacij	Uvesti se morajo formalne politike, postopki in kontrole prenosa, da se zaščiti prenos informacij pri uporabi vseh vrst komunikacijskih sredstev.
A.13.2.2.	Dogovori o prenosu informacij	Dogovori morajo obravnavati varen prenos poslovnih informacij med organizacijo in zunanjimi strankami.
A.13.2.3.	Elektronsko sporočanje	Informacije, vključene v elektronsko sporočanje, morajo biti ustrezno zaščitene.
A.13.2.4.	Dogovori o zaupnosti ali nerazkrivanju	Zahteve za dogovore o zaupnosti ali nerazkrivanju, ki odražajo potrebe organizacije za zaščito informacij, se morajo opredeliti, redno pregledovati in dokumentirati.
A.14.1.1.	Analiza in specifikacije zahtev varovanja informacij	Zahteve v zvezi z varovanjem informacij se morajo vključiti v zahteve za nove informacijske sisteme ali izboljšave obstoječih informacijskih sistemov.
A.14.1.2.	Varovanje aplikacijskih storitev v javnih omrežjih	Informacije, ki so vključene v aplikacijske storitve in se prenašajo prek javnih omrežij, se morajo zaščititi pred dejanji goljufij, spori glede pogodb ter pred nepooblaščenim razkritjem in premembami.
A.14.1.3.	Zaščita transakcij aplikacijskih storitev	Informacije, vključene v transakcije aplikacijskih storitev, se morajo zaščititi, da se preprečijo nepopoln prenos, napačno usmerjanje, nepooblaščene spremembe sporočil, nepooblaščeno razkritje, nepooblaščeno podvajanje ali ponavljanje sporočil.
A.14.2.1.	Varna razvojna politika	Pravila za razvoj programske opreme in sistemov se morajo določiti in uporabiti za razvoj znotraj organizacije.
A.14.2.2.	Postopki nadzora sprememb sistemov	Spremembe sistemov v okviru razvojnega življenjskega cikla se morajo nadzorovati z uporabo formalnih postopkov za nadzor sprememb.
A.14.2.3.	Tehnični pregled aplikacij po spremembah operacijskih sistemov	Ko se operacijske platforme spremenijo, se morajo poslovno kritične aplikacije pregledati in testirati, ter zagotoviti, da ni negativnega vpliva na organizacijsko poslovanje ali varnost.
A.14.2.4.	Omejitve pri spremembah programskih paketov	Spremembe programskih paketov se morajo poskušati preprečiti in omejiti na potrebne spremembe, vse spremembe pa se morajo strogo nadzorovati.
A.14.2.5.	Načela varnega sistemskega inženiringa	Načela za inženiring varnih sistemov se morajo vzpostaviti, dokumentirati, vzdrževati in uporabiti za vsa prizadevanja v zvezi z izvajanjem informacijskih sistemov.
A.14.2.6.	Varno razvojno okolje	Organizacije morajo vzpostaviti in ustrezno zaščititi varna razvojna okolja za prizadevanja v zvezi z razvojem in integracijo sistemov, ki zajemajo celoten življenjski cikel razvoja sistema.
A.14.2.7.	Zunanje izvajanje razvoja	Organizacija mora nadzorovati in spremljati aktivnost zunanjega razvoja sistema.
A.14.2.8.	Varnostno testiranje sistemov	Funkcionalnost varovanja informacij se mora testirati med razvojem.
A.14.2.9.	Prevzemno testiranje sistema	Za nove informacijske sisteme, posodobitve in nove različice se morajo vzpostaviti programi za prevzemno testiranje in z njim povezani kriteriji.
A.14.3.1.	Zaščita testnih podatkov	Testni podatki se morajo skrbno izbirati, ščititi in nadzorovati.
A.15.1.1.	Politika varovanja informacij za odnose z dobavitelji	Zahteve varovanja informacij za blažitev tveganj, povezanih z dostopom dobavitelja do sredstev organizacije, se morajo dogovoriti z dobaviteljem in dokumentirati.
A.15.1.2.	Obravnavanje varovanja v dogovorih z dobavitelji	Vse ustrezne zahteve varovanja informacij se morajo vzpostaviti in se o njih dogovoriti z vsakim dobaviteljem, ki lahko dostopa, obdeluje, hrani, sporoča ali zagotavlja informacijsko-tehnološke infrastrukturne komponente za informacije organizacije.
A.15.1.3.	Dobavna veriga informacijske in komunikacijske tehnologije	Dogovori z dobavitelji morajo vključevati zahteve za obravnavanje tveganj varovanja informacij, povezanih s storitvami informacijske in komunikacijske tehnologije ter dobavno verigo izdelka.
A.15.2.1.	Spremljanje in pregledovanje storitev dobaviteljev	Organizacije morajo redno spremljati, pregledovati in izvajati presoje izvajanja storitev dobavitelja.
A.15.2.2.	Upravljanje sprememb storitev dobaviteljev	Spremembe zagotavljanja storitev dobaviteljev se morajo upravljati, vključno z ohranjanjem in izboljševanjem obstoječih informacijskih varnostnih politik, postopkov in kontrol, pri čemer se morata upoštevati kritičnost poslovnih informacij, sistemov in vključenih procesov ter ponovna ocena tveganj.

A.16.1.1.	Odgovornosti in postopki	Vzpostaviti se morajo odgovornosti in postopki upravljanja za zagotovitev hitrega, uspešnega in urejenega odzivanja na dogodke in incidente varovanja informacij.
A.16.1.2.	Poročanje o dogodkih varovanja informacij	O dogodkih varovanja informacij se mora čim prej poročati vodstvu po ustreznih poteh.
A.16.1.3.	Poročanje o varnostnih slabostih varovanja informacij	Od zaposlenih in pogodbenikov, ki uporabljajo informacijske sisteme in storitve organizacije, se mora zahtevati, da zabeležijo vsako opaženo ranljivost varovanja informacij v sistemih ali storitvah ali sum nanjo ter poročati o njej.
A.16.1.4.	Ocena dogodkov varovanja informacij in odločitev o njih	Dogodki varovanja informacij se morajo oceniti ter se nato odločiti, ali se razvrstijo varnostni incidenti varovanja informacij.
A.16.1.5.	Odgovor na incidente varovanja informacij	Na incidente varovanja informacij se mora odgovoriti skladno z dokumentiranimi postopki.
A.16.1.6.	Učenje iz incidentov varovanja informacij	Znanje, pridobljeno pri analiziranju in odpravljanju incidentov varovanja informacij, se mora uporabiti za zmanjšanje možnosti ali vpliva prihodnjih incidentov.
A.16.1.7.	Zbiranje dokazov	Organizacija mora opredeliti in uporabiti postopke za prepoznavanje, zbiranje, pridobivanje in hrambo informacij, ki lahko služijo kot dokazi.
A.17.1.1.	Načrtovanje neprekinjenega varovanja informacij	Organizacija mora določiti svoje zahteve za varovanje informacij in neprekinjenost upravljanja varovanja informacij v neugodnih razmerah, npr. med krizo ali katastrofo.
A.17.1.2.	Izvajanje neprekinjenega varovanja informacij	Organizacija mora vzpostaviti, dokumentirati, izvajati in vzdrževati procese, postopke in kontrole za zagotavljanje zahtevane ravni neprekinjenega varovanja informacij v neugodnih razmerah.
A.17.1.3.	Preverjanje, pregledovanje in vrednotenje neprekinjenega varovanja informacij	Organizacija mora v rednih časovnih presledkih preverjati vzpostavljene in izvedene kontrole neprekinjenega varovanja informacij, da bi zagotovila veljavnost in uspešnost v neugodnih razmerah.
A.17.2.1.	Razpoložljivost naprav za obdelavo informacij	Naprave za obdelavo informacij se morajo izvesti v dovolj velikem številu za izpolnjevanje zahtev razpoložljivosti.
A.18.1.1.	Prepoznavanje veljavnih zakonskih in pogodbenih zahtev	Vse ustrezne zahteve zakonodaje, predpisov in pogodb ter pristop organizacije k izpolnitvi teh zahtev se morajo izrecno opredeliti, dokumentirati in sproti posodabljati za vsak informacijski sistem in organizacijo.
A.18.1.2.	Pravice intelektualne lastnine	Izvajati se morajo ustrezni postopki za zagotovitev skladnosti z zahtevami zakonodaje, predpisov in pogodb v zvezi s pravicami intelektualne lastnine ter uporabo lastniških programskih izdelkov.
A.18.1.3.	Zaščita zapisov	Zapisi se morajo zaščititi pred izgubo, uničenjem, ponarejanjem, nepooblaščenim dostopom in nepooblaščeno objavo v skladu z zahtevami zakonodaje, predpisov in pogodb ter poslovnimi zahtevami.
A.18.1.4.	Zasebnost in zaščita osebno določljivih informacij	Zagotoviti se morata zasebnost in zaščita osebno določljivih informacij, kot to zahtevajo ustrezna zakonodaja in predpisi.
A.18.1.5.	Uporaba kriptografskih kontrol	Kriptografske kontrole se morajo uporabljati v skladu z vsemi ustreznimi dogovori, zakoni in predpisi.
A.18.2.1.	Neodvisni pregled varovanja informacij	Pristop organizacije k upravljanju varovanja informacij in njegovo izvajanje (npr. cilji kontrole, kontrole, politike, procesi in postopki za varovanje informacij) se morata neodvisno pregledovati v načrtovanih časovnih presledkih ali kadar pride do bistvenih sprememb.
A.18.2.2.	Skladnost z varnostnimi politikami in standardi	Vodje morajo redno v okviru svojih odgovornosti pregledovati skladnost obdelave informacij in postopkov z ustreznimi varnostnimi politikami in standardi ter vsemi drugimi varnostnimi zahtevami.
A.18.2.3.	Pregled tehnične skladnosti	Redno se mora pregledovati skladnost informacijskih sistemov s politikami varovanja informacij in standardi organizacije.

Slika 5: Izjava o primernosti (SOA) ISO/IEC 27001 (varovanje podatkov)

1.5.7.2 ZVOP-1 in Uredba o varstvu posameznikov pri obdelavi osebnih podatkov

Zakon o varstvu osebnih podatkov določa, da morajo biti postopki in ukrepi za zavarovanje osebnih podatkov ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo. [9]

Že v sami zakonodaji je tako opredeljeno, da je potrebno ocenjevanje tveganj na področju zavarovanja osebnih podatkov, vendar večina organizacij tega ne izvaja. S prenovo zakona, ki je sedaj zapisan v obliki Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. april 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov za celotno Evropsko zvezo, se pričakuje, da bo področje ocenjevanja tvegaj bolj poudarjeno ter da bodo ukrepi zavarovanja dejansko sledili ocenjenim tveganjem. S tem pa se naj bi zmanjševali tudi stroški za ukrepe varovanja osebnih podatkov, saj se viri lahko načrtujejo le na področjih poslovanja, kjer je zaznano povišano tveganje.

1.5.7.3 ZVDAGA-A

Prav tako kot ZVOP-1 tudi Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih govori o tveganjih. Odstavek 17. člena, ki je pomemben za področje ocenjevanja tveganj, se glasi:

(1) Javnopravna oseba, ki bo zajemala ali hranila gradivo v digitalni obliki, ponudnik storitve zajema in hrambe oziroma spremljevalnih storitev in osebe, ki želijo uveljavljati veljavnost in dokazno vrednost svojega gradiva v skladu z določbami 31. člena ZVDAGA, morajo slediti naslednjim fazam priprave oziroma organizacije zajema in hrambe:

- priprava na zajem in hrambo,
- priprava in sprejem notranjih pravil za zajem in hrambo gradiva v digitalni obliki. [11]

Ta določila se povezujejo z Enotnimi tehnološkimi zahtevami, ki so podlaga za pripravo notranjih pravil in v katerih je navedeno:

1.5.7.4 ETZ 3.2.1.1

Organizacija mora izdelati oceno tveganja, s katero prepoznava in obvladuje tveganje, povezano s človeškimi viri, ter pravno, poslovno, organizacijsko, okoljsko in tehnološko tveganje, vezano na zajem oz. e-hrambo gradiva. Če organizacija vloži zahtevek za potrditev NP v državni arhiv, mora k vlogi priložiti tudi poročilo o izvedeni oceni tveganja. [12]

1.5.7.5 ZTP

Prav tako kot ZVOP in ZVDAGA tudi Zakon o tajnih podatkih določa področje ocenjevanja tveganj, kar je opredeljeno v Uredbi o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih.

(1) Vsak upravljalec sistema mora v postopku izdaje varnostnega dovoljenja za delovanje sistema pripraviti:

- načrt varovanja sistema, ki vsebuje opis sistema, načrt sestavin in povezav sistema, varnostne zahteve sistema, varnostna okolja, varnostne protiukrepe in varnostno upravljanje sistema,
- oceno varnostnih tveganj, ki vsebuje oceno trenutnega stanja sistema z oceno stopnje tveganja. [13]

1.5.7.6 ZEKOM-1

V Zakonu o elektronskih komunikacijah je opredeljena ocena tveganja kot ključni mehanizem pri zagotavljanju varnosti in omrežij, kar je opisano v 79. členu.

(1) Operaterji morajo sprejeti ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev, zlasti zaradi preprečevanja in zmanjševanja učinkov varnostnih incidentov na uporabnike in medsebojno povezana omrežja. Sprejeti ukrepi morajo ob upoštevanju stanja zagotoviti raven varnosti, primerno predvidenemu tveganju.

(2) Med ukrepe iz prvega odstavka spada tudi sprejem in izvajanje ustreznega varnostnega načrta, ki ga operater določi kot poslovno skrivnost.

(3) Varnostni načrt zajema najmanj:

- opredelitev vseh varnostnih tveganj znotraj operaterja, kakor tudi tistih zunaj operaterja, ki lahko ogrozijo delovanje javnega komunikacijskega omrežja oziroma lahko motijo delovanje javno dostopnih elektronskih komunikacijskih storitev, ki jih ta operater ponuja,
- opredelitev verjetnosti dogodka za vsa varnostna tveganja iz prejšnje alineje,
- opredelitev stopnje negativnih učinkov in posledic za delovanje javnega komunikacijskega omrežja in za javno dostopne komunikacijske storitve za vsa varnostna tveganja iz prve alineje. [14]

S tem vidimo, da je celotno področje informacijske varnosti vezano na ocenjevanje tveganj in sprejetje ustreznih ukrepov varovanja na podlagi tistih tveganj, ki so nesprejemljiva. Zato je smiselno, da organizacije temeljito ocenijo vsa tveganja, kar je najlažje z enostavno metodologijo in pripravljenimi katalogi groženj.

2 Pregled trga orodij za ocenjevanje tveganj

2.1 Zahteve trga

Organizacije, ki poskušajo izvesti oceno tveganja, se soočajo z naslednjimi izzivi:

- Nepoznavanje ali pomanjkljivo poznavanje metodologij ocen tveganja , kadar oceno tveganja izvajajo prvič.
- Pomanjkanje znanj za pripravo katalogov groženj in ranljivosti za področje ocenjevanja tveganj.
- Neustrezna izvedba kontrol, ki jih morajo upoštevati pri ocenjevanju tveganj (npr. ISO 9001 ali ISO/IEC 27001:2103 standard).
- Preveč podatkov, ki se generirajo pri ocenjevanju tveganj, na podlagi katerih je potrebno pripraviti ukrepe za zmanjšanje tveganj.
- Dosledna in enostavna primerjava posameznih ocen tveganja.
- Pomanjkanje dobrih praks ocenjevanja tveganj.

Potreba za ocenjevanje tveganj je posledica notranjih ali zunanjih zahtev.

- Notranje: organizacija želi postaviti sistem vodenja ali pokriti zahtevo lastnikov poslovnih procesov po izboljšanju poslovanja in s tem povezanega obvladovanja tveganj.
- Zunanje: organizacija mora zadostiti zakonskim zahtevam ali zahtevam nadzornikov organizacije, ki vključujejo oceno tveganja.

Večinoma izvajajo postopek ocenjevanja tveganj zunanji svetovalci. Organizacije, ki izvajajo oceno tveganja le kot posledico zunanjih dejavnikov, so zelo občutljive na strošek le-te in ne cenijo kakovosti izvedbe. Zanje svetovanje ni prava izbira, vendar druge možnosti ne obstajajo. Pričakuje se, da bo v prihodnosti večje povpraševanje po stroškovno učinkovitih rešitvah za oceno tveganja.

Organizacije, ki jih vodijo notranji dejavniki za ocenjevanje tveganj, na drugi strani večinoma zahtevajo, da ohranijo svoje obstoječe metodologije z namenom dosledne in enostavne primerjave ocen letnih tveganj. Tu nastaja problem svetovanja točno določenega zunanjega svetovalca, saj so pogosto specializirani samo za določene metodologije in menjava ponudnika ni možna oziroma je zelo otežena.

Kako lahko učinkovito in uspešno rešimo navedene težave? Področje ocenjevanja tveganj se v zadnjih letih izboljšuje – standardi so napisani, dobre prakse so priznane in ista načela in postopke se lahko uporablja za različne organizacije. Ker je izvedba ocene tveganja postala predvidljiv in ponovljiv proces, se pojavlja priložnost, da se izvedba lahko obvladuje s programsko opremo, ki vključuje dobre prakse ocenjevanja tveganj na vseh področjih poslovanja. Ocenjevanje tveganj se lahko podpre s priznanimi metodologijami, vključitvijo katalogov groženj in ranljivosti tveganj ter predlogi korektivnih ukrepov in ustvari potrebne zapise in dokumente, ki so potrebni zaradi zakonodaje, standardov ali zahtev nadzornikov.

Zahteve trga so, da mora informacijsko podprto orodje omogočati:

- enostavno in hitro prilagajanje na izbrano metodologijo ocenjevanja,
- ustrezne kataloge groženj in ranljivosti tveganj,
- hitro usposabljanje uporabnika za uporabo orodja (enostavnost izvedbe ocene tveganja),
- vključevanje vseh potrebnih metodologij za ocenjevanje tveganj.

2.2 Stanje na trgu

2.2.1 Pregled trga

Rezultati analize konkurence so prikazani v Tabeli 1. Rezultati analize konkurence so povzeti, kot sledi:

- Ciljni trgi:

Vsa orodja za ocenjevanje tveganj zahtevajo vključevanje strokovnjakov s področja ocenjevanja tveganj. Nobeno orodje ni primerno za uporabo na način, da bi ga lahko upravljal nekdo, ki nima izkušenj z ocenjevanjem tveganj. Kot posledica tega so ciljni trgi skoraj izključno velike organizacije.

- Metodologije:

Večina orodij je omejena zgolj na posamezne metodologije (večina na ocenjevanje tveganj na področju IT), nobeno ne pokriva celovitega področja kakovosti oziroma poslovanja organizacij.

- Poslovni model:

V večini primerov je programska oprema licencirana na uporabnika. Zaradi cen je na trgu skoraj izključno namenjena velikim organizacijam.

- Cene:

Cene za licenco uporabnika znašajo od 1200 evrov do 4000 EUR na licenco (razen v primeru RealISMS, ki se omejuje na področje ISO/IEC 27001 in ne omogoča ocenjevanja tveganj poslovanja).

	Konkurenčna orodja za ocenjevanje tveganj									
	RM Stream	Secura	Counter Measures	Info.rm	Modulo	Proteus	SBR	vsRisk	RealISMS	RM Studio
Ciljni trgi										
Strokovnjaki OT	x	x	x		x	x	x	x	x	x
Majhne organizacije	x					x			x	x
Srednje velike organizacije	x	x		x		x		x	x	x
Velike organizacije	x	x	x	x	x	x	x	x	x	x
Poslovni model										
Zastonj	x *									
Uporabniška licenca	x	x		x			x	x		x
Mesečni najem			x		x				x	
Ni znano						x				
Cena	0 EUR, 300 EUR modul	4.000 EUR	150 EUR / mesec	4.000 EUR	Ni znana cena.	Ni znana cena.	10.000 EUR	1.200 EUR	40 EUR / mesec	2.500 EUR
*- platforma zastonj za enega uporabnika do 3.000 EUR na licenco, posamezni moduli z različnimi metodologijami pa od 300 EUR dalje										

Slika 6: Povzetek analize konkurence

2.2.2 Konkurenčna orodja

V analizi konkurenčnih orodij smo izbrali naslednje organizacije, ki izstopajo, bodisi zaradi popolnosti in funkcionalnost izdelka ali zaradi poslovnega modela:

- RM Stream
- Modulo
- RM studio
- SBR
- INFO.RM

Primerjalna matrika je predstavljena v Tabeli 2 na koncu tega poglavja.

RM Stream

RM Stream je izdelek podjetja Acuity iz Velike Britanije. Njihova prednost je, da nudijo programsko opremo, ki je popolnoma prilagodljiva - lahko določite lastno metodologijo, vire in poročila. Programska oprema zato deluje kot platforma in je brezplačna za enega uporabnika, vendar je za organizacije plačljiva do 2.500 EUR. Glavna dejavnost podjetja je, da nudi upravljanje s tveganji na vseh področjih poslovanja. Posamezen modul stane 300 EUR. Moduli so predpripravljeni za posamezno metodologijo. Kot glavno konkurenčno prednost je smiselno izpostaviti brezplačnost za enega uporabnika.

Modulo

Modulo je izdelek podjetja Modulo iz Brazilije. Njihova glavna konkurenčna prednost je pokrivanje različnih področij upravljanja s tveganji od ISO/IEC 27001 do Basel III, HIPAA in Sarbanes-Oxley. S tem so poznani kot celovito GRC orodje za večje organizacije.

RM Studio

RM Studio je izdelek podjetja Stiki z Islandije. Njihova glavna konkurenčna prednost je orodje, ki je enostavno za uporabo in usmerjeno v pokrivanje zahtev ISO/IEC 27001 certificiranja.

SBR

SBR je izdelek slovenskega podjetja Netis d.o.o. To podjetje nima posebnega poslovnega modela, konkurenčna prednost je predvsem uporaba slovenskega jezika in prilagodljivost metodologije ocenjevanja tveganj za posameznega kupca.

INFO.RM

Info.RM je izdelek slovenskega podjetja Kvali.dat. Podjetje nima posebnega poslovnega modela, konkurenčna prednost je predvsem uporaba slovenskega jezika in cenovno ugodno orodje, ki pokriva predvsem ISO/IEC 27001.

Orodje	RM Stream	Modulo	RM Studio	SBR	Info.RM
Metodologija					
Procesni pristop	da	da	da	da	da
Identifikacija tveganj	da	da	da	da	da
Kontrole zmanjševanja tveganj	da	da	da	da	da
Upravljanje tveganj	da	da	da	da	da
Definiran nivo tveganja	da	da	da	da	da
Vprašalniki za oceno tveganja	da	ne	da	da	ne
Definiranje politik na podlagi ocene tveganja	ne	ne	ne	ne	ne
Vsebina					
Vzorci virov	da	ne	da	da	da
Prilagajanje virov	da	da	da	da	da

Vzorci groženj	da	da	da	da	da
Vzorci ranljivosti	da	da	da	da	da
Matrika ocene tveganja	da	ne	da	da	da
Analiza					
Ključna tveganja	da	da	da	da	da
Vpliv ukrepov	da	da	da	da	da
Primerjava tveganj	da	da	da	ne	ne
Revizijska sled	da	da	da	da	da
Poročanje					
Vzorci poročil	da	da	da	da	da
Prilagodljivost poročil	da	da	da	ne	ne
Grafi	da	da	da	da	ne
Delovanje					
Klient na delovni postaji	da	da	da	ne	da
Strežniška postavitev	da	da	da	da	da
Oblačna storitev	ne	da	ne	ne	ne
Večjezičnost	ne	da	da	ne	ne
Večuporabniški vmesnik	ne	ne	ne	ne	ne
Upravljanje s pravicami uporabnikov	da	da	da	da	da
Oddaljena pomoč	da	da	da	ne	ne
Brezplačni poizkus uporabe	da	da	da	da	da
OS	Microsoft	neodvisen	Microsoft	neodvisen	neodvisen
Uporaba na mobilnih napravah	da	da	da	ne	ne

Slika 7: Primerjalna tabela orodij za ocenjevanje tveganj

2.3 Identifikacija poslovnih priložnosti

Poslovna priložnost	Področje	Pojasnilo
Segment trga	Tveganja poslovanja (npr. ISO 9001)	Posamezno področje je preveč ozko specializirano in prodaja v takšnem obsegu je tvegana.
	Tveganja upravljanja s podatki (npr. Uredba o varstvu osebnih podatkov)	
	Tveganja upravljanja z gradivom (npr. ZVDAGA)	
Velikost organizacije	Majhne organizacije	Rešitev za majhne organizacije, kjer ni zaposlenih strokovnjakov za ocenjevanje tveganj.
Poslovni model	Nizka cena	Dolg prodajni cikel povezan z visoko ceno programske opreme predstavlja visoko tveganje.
	Mesečni najem	

Slika 8: Primerjalna tabela orodij za ocenjevanje tveganj

3 Ciljni trgi programske opreme OTO – Ocena tveganja organizacije

3.1 Ciljni trgi

Identificirana sta dva ciljna trga:

- ocenjevanje tveganj po vseh segmentih s poudarkom na poslovanju,
- ocenjevanje tveganj v majhnih organizacijah zaradi zakonskih zahtev.

Ciljni odjemalci na prvem ciljnem trgu:

- strokovnjaki, zaposleni v srednje velikih organizacijah,
- zunanji svetovalci.

Ciljni odjemalci na drugem ciljnem trgu:

- direktorji organizacij,
- administrativno osebje,
- zunanji svetovalci.

3.2 Vrednost posameznega odjemalca

Spodnja tabela prikazuje podatke o tekočih stroških strank za izvedbo ocenjevanja tveganj brez uporabe informacijsko podprtega orodja.

Da bi dobili izračunano vrednost prihrankov, je predpostavka, da stane delodajalca ocenjevanje tveganj okvirno 1.500 EUR na leto za izvedenih 60 delovnih ur. Z uporabo informacijsko podprtega orodja se prihrani 50 delovnih ur na leto, skupni letni prihranek za kupca je 1.250 EUR letno.

Aktivnost	**Stroški (delovne ure) brez informacijsko podprtega orodja**	**Stroški (delovne ure) z informacijsko podprtim orodjem**
Posodabljanje katalogov groženj in ranljivosti	4	1
Posodabljanje metodologij	6	0
Vpis procesov	8	2
Priprava poročil	10	1
Upravljanje z ukrepi	10	2
Poročanje zaposlenim	10	2
Nadzor nad ukrepi	12	2
Skupno	**60**	**10**

Slika 9: Prihranek časa z uporabo orodja za ocenjevanje tveganj

Stroški in prihranki				
Strošek ocenjevanja tveganj	1.500 EUR / leto			
Strošek nakupa	1.980 EUR + 198 EUR vzdrževanja / leto			
Prihranek na leto	-674 EUR	1.302 EUR	1.302 EUR	1.302 EUR
Strošek najema	960 EUR / leto			
Prihranek na leto	540 EUR	540 EUR	540 EUR	540 EUR

Slika 10: Stroški in prihranki za stranko

3.3 Poslovni model in prihodki

3.3.1 Ciljni trgi – tipi odjemalcev

Majhne in srednje velike organizacije:

- majhne organizacije (zahteve zakonodaje in standardov),
- srednje velike organizacije (ocenjevanje tveganj po vseh segmentih s poudarkom na poslovanju).

3.3.2 Ciljni trgi – geografska lokacija

Ciljni trgi so EU in JV Evropa (večjezičnost vgrajena v programsko opremo).

3.3.3 Poslovni model 1 – nakup licence in storitve za stranke

Nakup licence obsega:

- programsko opremo za ocenjevanje tveganj,
- 1x modul (npr. ISO 9001),
- vzdrževanje (podpora uporabnikom, prilagoditev katalogov groženj in ranljivosti).

Licenca	Stroški
Uporabnik	1.980 EUR
Modul	250 EUR (1x modul brezplačno)
Vzdrževanje	198 EUR (prvo leto brezplačno, ni pogoj za nakup)

Slika 11: Stroški za stranko

3.3.4 Poslovni model 2 – najem licence in storitve za stranke

Najem licence obsega:

- programsko opremo za ocenjevanje tveganj za določen čas,
- 1x modul (npr. ISO 9001) za določen čas,
- vzdrževanje (podpora uporabnikom, prilagoditev katalogov groženj in ranljivosti).

Licenca	Stroški
Uporabnik	80 EUR mesečno
Modul	10 EUR mesečno
Vzdrževanje	0 EUR

Slika 12: Stroški za stranko

3.3.5 Prihodki

Prihodki				
Poslovni model 1	1.980 EUR + 198 EUR vzdrževanja / leto / stranko			
Nove stranke v 2016 -2020	10	50	100	200
Prihodki	19.800 EUR	100.980 EUR	209.880 EUR	427.680 EUR

Slika 13: Prihodki nakupa

Prihodki				
Poslovni model 1	960 EUR + 120 EUR najema / leto / stranko			
Nove stranke v 2016 -2020	10	50	100	200
Prihodki	10.800 EUR	64.800 EUR	172.800 EUR	388.800 EUR

Slika 14: Prihodki najema

4.1.1 Potrebne funkcionalnosti programske opreme OTO – Ocena tveganja organizacije

Programska oprema omogoča več, kot je potrebno zaradi zahtev zakonodaje ali standardov, saj poenostavi celotno ocenjevanje tveganj z naslednjimi mehanizmi, kar pomeni prednost pred konkurenčnimi orodji:

- enostavno prijavo uporabnika v programsko opremo z enoznačnim uporabniškim imenom (in geslom),
- vpogled v nabor modulov,
- namenski administrativni modul upravljanja z ocenami tveganj,
- vpogled v okolje organizacije (poslovni procesi, organizacijska struktura, viri),
- določitev nivoja ocene tveganja (organizacija, posamezna organizacijska enota, poslovni procesi, posamezni viri),
- vpogled v vire organizacije (značilnosti vira in finančna ocena vira),
- vpogled v nabor ocen tveganj,
- izbiro posameznega dela ocene tveganja (glede na vlogo uporabnika),
- izračun povprečne ocene tveganja in primerjava med posameznimi ocenami tveganj,
- pripravo ukrepov za zmanjšanje tveganj (izbira posameznih elementov med ukrepi oziroma, če ni možna izbira - vpisovanje podatkov),
- pregled vseh ukrepov za zmanjšanje tveganj (glede na vlogo uporabnika),
- določanje odgovornih oseb za tveganja (glede na vlogo uporabnika),
- opozarjanja pooblaščenih oseb za ukrepe glede stanja ukrepa (v čakanju, izvedeno, itd.),
- opozarjanje pooblaščenih oseb za stalne oziroma ponavljajoče ukrepe,
- opozarjanje odgovornih oseb za tveganja glede izvedbe posameznih ukrepov,
- opozarjanje varnostnega inženirja oziroma skrbnikov sistemov vodenja o izvedbi ukrepov,
- pregled stanja izvedenih ukrepov in zmanjšanih tveganj (glede na vlogo uporabnika),
- povezovanje ocen tveganja med seboj in primerjave rezultatov,
- izpis ocene tveganj v standardnih formatih in vzorčnih obrazcih.

4.2 Upravičenost programske opreme

Upravičenost programske opreme je vidna predvsem s stališča možne uporabe različnih deležnikov in s tem poenostavljenega procesa ocenjevanja tveganj:

- Vodstvo organizacij – uporabljali bodo predvsem funkcijo nadzora nad ukrepi oziroma zmanjševanjem tveganj. 1x letno bodo pregledali oceno tveganja skupaj z varnostnim inženirjem oziroma skrbnikom sistema vodenja. Dostop morajo imeti do celovitega pregleda tveganj ter izvajanja ukrepov v celotni organizaciji.
- Lastniki procesov – vsaj 1x letno bodo sodelovali pri pripravi ocene tveganja, odgovorni bodo za posamezno tveganje oziroma bodo določali, kdo bo izvajal posamezen ukrep. Dostop morajo imeti do pregleda tveganj in izvajanja ukrepov v svojem procesu.
- Izvajalci ukrepov – obveščeni morajo biti o izvedbi posameznega ukrepa, za katerega so zadolženi.
- Nadzorniki – iz ukrepov morajo videti izboljševanje poslovanja organizacije. Dostop morajo imeti do celovitega pregleda tveganj ter izvajanja ukrepov v celotni organizaciji.

4.3 Razlika programske opreme OTO od konkurenčnih orodij

Programska oprema OTO predstavlja celovito orodje za obvladovanje tveganj, zato zagotavlja obvladovanje tveganj na vseh področjih poslovanja. Zaradi različnih pristopov k ocenjevanju tveganj je programska oprema sestavljena iz osnovnega modula, ki predstavlja ogrodje programske opreme, v katerem se odvija administracija podatkov, vlog uporabnikov, vključitev v obstoječ informacijski sistem (npr. mrežno povezovanje), v povezanih modulih pa so nabori metodologij za različna področja ocenjevanja tveganj.

Programska oprema omogoča izvedbo ocene tveganja s čim manj uporabniškega vnosa podatkov in čim manj uporabnikovega dela (posameznih klikov na možnosti, izbire podatkov).

Programska oprema podaja možne odgovore na uporabnikove vnose podatkov (predpripravljeni odgovori oziroma izračuni tveganj).

Programska oprema omogoča nadgrajevanje brez podrobnejšega poznavanja IT tehnologij.

Programska oprema zahteva kar najmanj strojne zmogljivosti (enostavne metodologije, malo podatkov, ki jih vnaša uporabnik, malo uporabnikov) oziroma je lahko najem storitve v oblaku. Programska oprema omogoča opozarjanje uporabnikov (znotraj aplikacij in preko e-pošte).

Najpomembnejše razlike s konkurenčnimi orodji so naslednje:

- uporaba v različnih operacijskih sistemih,
- uporaba sporočilnih sistemov (e-pošta),
- skladnost namestitev v različnih okoljih organizacij (namestitev na delovni postaji ali strežniška namestitev),
- neuporaba plačljivih delov programske opreme tretjih strank.

4.4 Funkcionalnost programske opreme

Ključne lastnosti orodja so definirane s stališča uporabnika. Vse zahteve so ocenjene glede na potrebne funkcije, ki jih orodje potrebuje s prioritetami: nizka, srednja, visoka. Vse prioritete, ki so definirane kot visoke, so ključne za tržno uspešnost programske opreme. Prioritete, ki so definirane kot srednje, so ključne za uspešnost nadaljnjih verzij programske opreme, prioritete, ki so definirane kot nizke, pa se bodo vpeljale, v kolikor bo to zahtevalo več uporabnikov.

ID	Prioriteta	Značilnost
PR #1	Visoka	Tip uporabnikov: - lastnik procesa - vodstvo - izvajalec ukrepov - nadzornik
Ciljni trg:		majhne in srednje velike organizacije
Opis:		hiter vpogled v rezultate ocene tveganja in ukrepe

ID	Prioriteta	Značilnost
PR #2	Visoka	Tip uporabnikov: - vodstvo
Ciljni trg:		majhne in srednje velike organizacije
Opis:		hiter pregled najvišjih tveganj ter opis stroškov ukrepov

ID	Prioriteta	Značilnost
PR #3	Visoka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		majhne in srednje velike organizacije
Opis:		vsa tveganja organizacije v enem orodju

ID	Prioriteta	Značilnost
PR #4	Visoka	Tip uporabnikov: - vodstvo - nadzornik
Ciljni trg:		majhne in srednje velike organizacije
Opis:		primerjava višine tveganj skozi leta izvajanja ocenjevanja tveganj

ID	Prioriteta	Značilnost
PR #5	Visoka	Tip uporabnikov: - vodstvo - izvajalec ukrepov - nadzornik
Ciljni trg:		majhne in srednje velike organizacije
Opis:		pregled statusa izvajanja ukrepov

ID	Prioriteta	Značilnost
PR #6	Srednja	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		dostop do ocene tveganja s katerekoli lokacije

ID	Prioriteta	Značilnost
PR #7	Visoka	Tip uporabnikov: - lastnik procesa
Ciljni trg:		majhne in srednje velike organizacije
Opis:		orodje vsebuje kataloge groženj in ranljivosti

ID	Prioriteta	Značilnost
PR #8	Visoka	Tip uporabnikov: - lastnik procesa
Ciljni trg:		srednje velike organizacije
Opis:		vključen mora biti procesni pristop

ID	Prioriteta	Značilnost
PR #9	Srednja	Tip uporabnikov: - lastnik procesa - izvajalec ukrepov
Ciljni trg:		majhne organizacije
Opis:		orodje na enostaven način vodi skozi oceno tveganja

ID	Prioriteta	Značilnost
PR #10	Srednja	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		definiranje lastne metodologije

ID	Prioriteta	Značilnost
PR #11	Nizka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		definiranje novih katalogov groženj

ID	Prioriteta	Značilnost
PR #12	Visoka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		majhne in srednje velike organizacije
Opis:		ocena tveganja mora biti opravljena v 30 minutah

ID	Prioriteta	Značilnost
PR #13	Visoka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		ukrepi so lahko določeni različnim zaposlenim

ID	Prioriteta	Značilnost
PR #14	Srednja	Tip uporabnikov: - nadzornik
Ciljni trg:		majhne in srednje velike organizacije
Opis:		izpis v formatu .pdf

ID	Prioriteta	Značilnost
PR #15	Visoka	Tip uporabnikov: - lastnik procesa - nadzornik
Ciljni trg:		majhne in srednje velike organizacije
Opis:		izvedba kontrolnih vprašalnikov (npr. SoA itd.)

ID	Prioriteta	Značilnost
PR #16	Nizka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		vnos definiranih metodologij

ID	Prioriteta	Značilnost
PR #17	Nizka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		revizijske sledi

ID	Prioriteta	Značilnost
PR #18	Nizka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		izračun stroškov ukrepov

ID	Prioriteta	Značilnost
PR #19	Srednja	Tip uporabnikov: - lastnik procesa
Ciljni trg:		majhne in srednje velike organizacije
Opis:		enostavnost nadgradnje oziroma dopolnitve orodja z novimi moduli
ID	Prioriteta	Značilnost
PR #20	Nizka	Tip uporabnikov: - lastnik procesa - vodstvo
Ciljni trg:		srednje velike organizacije
Opis:		arhiviranje podatkov

Slika 15: Funkcije, potrebne za tržno uspešnost

5 Razvoj programske opreme OTO – Ocena tveganja organizacije - specifikacije

5.1 Namen programske opreme

Na podlagi zahtev standardov in zakonodaje je bila razvita programska oprema, ki pokriva vse zahteve ocenjevanja tveganj. Namen programske opreme OTO – Ocena tveganja organizacije je obvladovanje tveganj v celoti – določanje okolja, doseganja ciljev, ocenjevanje tveganj in izvajanje vseh ukrepov v organizaciji ter 'ISO' podpora vodstvu.

5.2 Obseg programske opreme

Programska oprema mora obsegati vsa področja obvladovanja tveganj za vse vrste organizacij, metodologij ocene tveganj ali značilnosti poslovanja oziroma sisteme vodenja (ISO). Cilj programske opreme je zagotoviti enostaven vpogled v ocenjevanje tveganj, odprtost programske opreme z možnim dopolnjevanjem vseh deležnikov ter enostavnost uporabe za uporabnike, ki ne poznajo IT tehnologij.

Vsak deležnik mora dobiti vpogled v svoje zahteve (ocena tveganja, seznam ukrepov, izvajanje ukrepov, opozorila v določenih terminih) z dostopom, ki je enoznačen za posameznika in brez težav z uporabo omejevalnikov dostopa (npr. gesla). Programska oprema mora omogočati izvedbo ocene tveganj v kratkem času brez podrobnejšega poznavanja posameznih tveganj.

Programska oprema mora biti nameščena brez podrobnejšega poznavanja IT tehnologij.

Programska oprema mora biti zmožna kasnejšega nadgrajevanja, tako tehničnega (npr. prilagoditve na različna okolja – operacijske sisteme, posodobitve aplikacije) kot vsebinskega (dopolnitve metodologije, modulov in zapisov).

Programska oprema mora omogočati izvoz podatkov v standardnih formatih v vzorčne obrazce.

5.3 Definicije, kratice in okrajšave

Programska oprema mora pokrivati področja, ki so opredeljena z naslednjimi definicijami, kraticami in okrajšavami:

- Ocena tveganja – izračun tveganja na podlagi vhodnih podatkov, ki jih organizacija izbere iz nabora podatkov v programski opremi oziroma vpisanih podatkih.
- Metodologija – način izračuna tveganj, ki je podan za vsako oceno tveganja posebej in se lahko izbere iz nabora metodologij v programski opremi ali lastnem vpisu metodologije.
- Tveganje – verjetnost dogodka, ki lahko izrabi ranljivost organizacije in povzroči škodo, nezgodo ali izgube in se ga da preprečiti z ustreznimi ukrepi.
- Modul – posamezen segment programske opreme, ki ima svoje značilnosti zaradi specifičnega ocenjevanja tveganj za posamezno področje.
- Tveganje kakovosti (ISO 9001) – tveganje, ki nastane zaradi zagotavljanja ustreznosti oziroma kakovosti posameznih produktov in storitev, ki jih organizacija ponuja.
- Tveganje poslovanja (podsklop ISO 9001) – tveganje, ki nastane pri poslovanju organizacije in se vodi v registru tveganj ter se ocenjuje z vidika finančne izgube oziroma škode pri poslovanju.
- Tveganje varstva pri delu (podsklop ISO 9001) – tveganje, ki nastane v delovnem procesu oziroma pri izvajanju dela v organizaciji.
- Tveganje okoljskih ravnanj (podsklop ISO 9001) – tveganje, ki nastane zaradi uporabe okoljsko nesprejemljivih snovi oziroma obdelave odpadkov v organizaciji.
- Tveganje varovanja informacij (ISO/IEC 27001) – tveganje, ki nastane ob uporabi informacijskih tehnologij oziroma ob pripravi, obdelavi, hrambi in uničevanju/izbrisu podatkov.
- Tveganje varstva osebnih podatkov – Uredba (podsklop ISO/IEC 27001) – tveganje, ki nastane zaradi potreb po varnosti osebnih podatkov.

- Tveganje varstva telekomunikacij – ZEKOM-1 (podsklop ISO/IEC 27001) – tveganje, ki nastane zaradi potreb po neprekinjenem delovanju posameznih storitev organizacije.
- Tveganje varstva dokumentarnega in arhivskega gradiva - ZVDAGA (podsklop ISO/IEC 27001) – tveganje, ki nastane zaradi potreb po varstvu gradiva v elektronski obliki.
- Tveganje varstva tajnih podatkov – ZTP (podsklop ISO/IEC 27001) – tveganje, ki nastane zaradi potreb po varovanju tajnih podatkov.
- Ukrepi – ravnanja, ki omogočajo, da je posamezno tveganje zmanjšano na sprejemljivo raven.

Širši nabor definicij, kratic in okrajšav se najde v podrobnejših specifikacijah za posamezen modul programske opreme v prilogah.

5.4 Opis programske opreme

Programska oprema predstavlja celovito orodje za obvladovanje tveganj, zato mora zagotavljati obvladovanje tveganj na vseh področjih poslovanja, kjer je potrebno ocenjevati tveganja zaradi zahtev zakonodaje ali standardov.

Programska oprema mora omogočati samostojno postavitev znotraj obstoječega informacijskega sistema ter dostop za vse deležnike brez tehničnih omejitev zaradi okolja organizacije (različni operacijski sistemi).

Zaradi značilnosti programske opreme, ki ne bo pogosto uporabljena oziroma ne predstavlja ključne programske opreme za izvajanje dela v organizaciji, je najpomembnejša enostavnost in hiter dostop do rezultatov, ki omogoča ustrezno ukrepanje.

Osnovne zahteve za programsko opremo so možna implementacija različnih metodologij, vpis podatkov več uporabnikov, več modulov za ocenjevanje različnih tveganj, združevanje tveganj po značilnostih in ukrepih, obveščanje uporabnikov o ukrepih (pripravljenih, izvajanju, izvedenih, neizvedenih).

Programska oprema mora diferencirati dostop posameznih uporabnikov glede na vlogo, ki jo imajo pri izvajanju ocene tveganj.

Programska oprema mora omogočati izvoz podatkov v formatih, ki se lahko preberejo in izpišejo v različnih operacijskih sistemih oziroma aplikacijah za obravnavo.

Programska oprema mora omogočati izvedbo ocene tveganja s čim manj uporabniškega vnosa podatkov in čim manj uporabnikovega dela (posameznih klikov na možnosti, izbiri podatkov).

Programska oprema mora omogočati možne odgovore na uporabnikove vnose podatkov (predpripravljeni odgovori oziroma izračuni tveganj).

Programska oprema mora omogočati nadgrajevanje brez podrobnejšega poznavanja IT tehnologij.

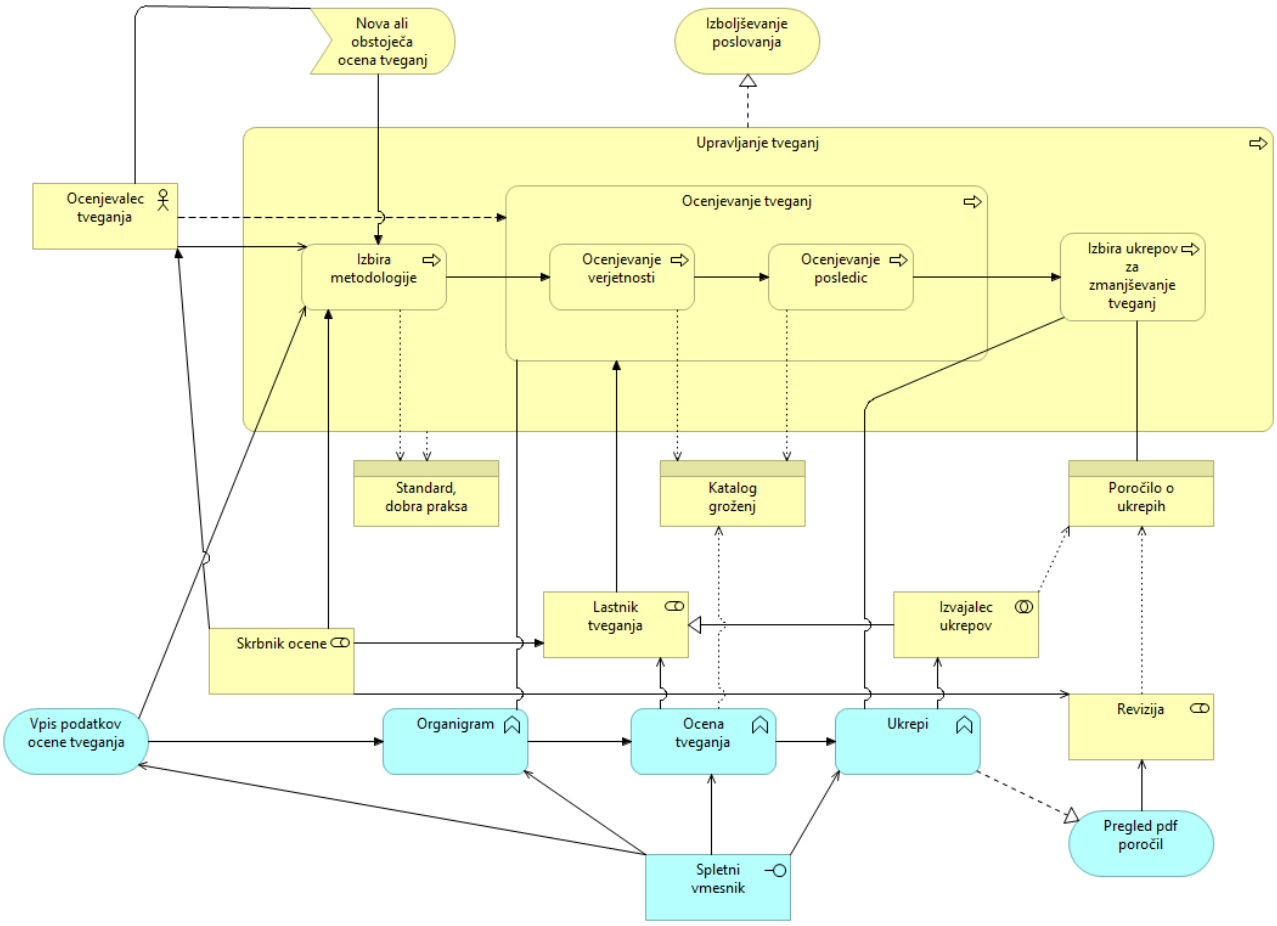
5.5 Funkcionalnost programske opreme

Programska oprema mora omogočati:

- prijavo uporabnika v programsko opremo z enoznačnim uporabniškim imenom (in geslom),
- vpogled v nabor modulov,
- administrativni modul,
- vpogled v okolje organizacije (poslovni proces, organizacijska struktura, viri),
- določitev nivoja ocene tveganja (organizacija, posamezna organizacijska enota, poslovni proces, posamezni viri),
- vpogled v vire organizacije (značilnosti vira in finančna ocena vira),
- vpogled v nabor ocen tveganj,
- izbiro posamezne ocene tveganja,

- izbiro posameznega dela ocene tveganja (glede na vlogo uporabnika),
- izračun ocene tveganja za posamezne vire oziroma značilnosti delovanja organizacije (izbira posameznih elementov v oceni oziroma, če ni možna izbira, vpisovanje podatkov),
- izračun povprečne ocene tveganja in primerjavo med posameznimi ocenami tveganj, pripravo ukrepov za zmanjšanje tveganj (izbira posameznih elementov med ukrepi oziroma, če ni možna izbira, vpisovanje podatkov),
- pregled vseh ukrepov za zmanjšanje tveganj (glede na vlogo uporabnika),
- povezovanje ukrepov med ocenami tveganj,
- določanje odgovornih oseb za tveganja (glede na vlogo uporabnika),
- opozarjanja pooblaščenih oseb za ukrepe glede stanja ukrepa (v čakanju, izvedeno, itd.),
- opozarjanje pooblaščenih oseb za stalne oziroma ponavljajoče ukrepe,
- opozarjanje odgovornih oseb za tveganja glede izvedbe posameznih ukrepov,
- opozarjanje varnostnega inženirja oziroma skrbnikov sistemov vodenja o izvedbi ukrepov,
- pregled stanja izvedenih ukrepov in zmanjšanih tveganj (glede na vlogo uporabnika),
- povezovanje ocen tveganja med seboj in primerjave rezultatov,
- izpis ocene tveganj v standardnih formatih in vzorčnih obrazcih.

5.6 Osnovni model delovanja programske opreme



Slika 6: Delovanje programske opreme

5.7 Uporabniki in karakteristike programske opreme

Uporabniki programske opreme so naslednji:

Varnostni inženirji oziroma skrbniki sistemov vodenja – programsko opremo se uporablja večkrat letno kot nadzor nad izvajanjem ukrepov in zmanjševanjem tveganj. Vsaj 1x letno se izvede oceno tveganja oziroma delegira izvajanje posameznih ocen tveganja lastnikom procesov/vodjem oddelkov. Njihova dolžnost bo predstavitev tveganj vodstvu organizacij, nadzornikom ali revizorjem. Potreben je dostop do administracije programske opreme, celovitega pregleda tveganj ter izvajanja ukrepov.

Vodstvo organizacij – uporablja se predvsem funkcijo nadzora nad ukrepi. 1x letno se pregleda oceno tveganja skupaj z varnostnim inženirjem oziroma skrbnikom sistema vodenja. Potreben je dostop do celovitega pregleda tveganj ter izvajanja ukrepov.

Lastniki poslovnih procesov/vodje oddelkov – vsaj 1x letno sodelujejo pri pripravi ocene tveganja, odgovorni so za posamezno tveganje oziroma določajo, kdo bo izvajal posamezen ukrep. Potreben je dostop do pregleda tveganj in izvajanja ukrepov v svojem procesu/oddelku.

Zaposleni/pogodbeni sodelavci – obvestiti jih je potrebno o izvedbi posameznega ukrepa, za katerega so zadolženi.

Nadzorniki – iz ukrepov se mora predvidevati izboljšanje poslovanja organizacije. Potreben je dostop do celovitega pregleda tveganj ter izvajanja ukrepov.

Revizorji – videti morajo delovanje sistemov vodenja oziroma aktivno izvajanje ukrepov. Potreben je dostop do celovitega pregleda tveganj ter izvajanja ukrepov.

Ključni element za vse uporabnike je sporočanje o tveganjih in ukrepih iz programske opreme.

5.8 Okolje delovanja programske opreme

Programska oprema mora delovati v različnih informacijskih sistemih organizacij (operacijski sistemi, mreža, strojna oprema). Programska oprema mora biti nameščena v okolje organizacije, kar pomeni bodisi strežniška infrastruktura bodisi posamezna delovna postaja.

5.9 Omejitve pri načrtovanju in implementaciji

Programska oprema mora porabiti kar najmanj strojne zmogljivosti (enostavne metodologije, malo podatkov, ki jih vnaša uporabnik, malo uporabnikov). Programska oprema mora omogočati opozarjanje uporabnikov.

Omejitve so naslednje:

- uporaba v različnih operacijskih sistemih (oz. najmanj v MS okolju),
- uporaba sporočilnih sistemov,
- skladnost namestitev v različnih okoljih organizacij (namestitev na delovni postaji ali strežniška namestitev),
- neuporaba plačljivih delov programske opreme tretjih strank.

5.10 Uporabniška dokumentacija

Pomoč za uporabnike se mora nahajati zraven posameznega okna/elementa v programski opremi kot možnost (npr. pojavno okno, če uporabnik to zahteva) in kot splošna navodila ob prijavi v programsko opremo.

5.11 Predpostavke in odvisnosti

Programska oprema ima nekaj predpostavk, ki se morajo upoštevati pri izgradnji:

- Programska oprema mora omogočati delo več uporabnikom hkrati.
- Programska oprema ne sme vsebovati plačljivih delov programske opreme tretjih strank.
- Programska oprema mora omogočati nadgradnje (tehnične in vsebinske) brez ponovne namestitve celotne programske opreme.

- Programska oprema mora biti povezljiva s programsko opremo za obveščanje uporabnikov (npr. e-pošta).
- Programska oprema mora zagotavljati vsebinsko večjezičnost.
- Programska oprema mora omogočati dodajanje modulov in metodologij.

6 Uporabniške zahteve

6.1 Zahteve glede vmesnikov programske opreme

6.1.1 Uporabniški vmesniki

Programska oprema mora imeti naslednja prikazovalna okna:

- Prijavo uporabnika v programsko opremo z enoznačnim uporabniškim imenom (in geslom)
    - Prvo okno omogoča opis programske opreme in prijavo.
- Vpogled v nabor modulov
    - Po vpisu uporabnika, se glede na vlogo prikažejo možni moduli za ocene tveganja. Uporabnik izbere, kateri modul bo uporabljal.
- Administrativni modul
    - To je modul, kjer varnostni inženir ali skrbnik sistemov vodenja izbira in pripravi metodologijo za ocene tveganja, dobi informacijo o drugih modulih, določi pravice v programski opremi, ureja nastavitve sporočilnega sistema (npr. e-pošta), določa elemente posamezne ocene tveganja.
- Vpogled v okolje organizacije (poslovni procesi, organizacijska struktura, viri)
    - To je modul, kjer uporabnik vidi organizacijo, njene poslovne procese, organizacijsko strukturo in vire, ki jih ima z namenom doseganja ciljev.
- Določitev nivoja ocene tveganja (organizacija, posamezna organizacijska enota, poslovni procesi, posamezni viri)
    - V modulu uporabnik vidi organizacijo, določi, kako se bo izvajala ocena tveganja oziroma, kateri poslovni procesi, organizacijske enote in viri bodo vključeni v posamezni oceni tveganja.
- Vpogled v vire organizacije (značilnosti vira in finančna ocena vira)
    - V modulu, kjer uporabnik vidi organizacijo, je viden tudi posamezen vir in značilnosti, ki so pomembni za ocenjevanje tveganj (v katero skupino virov sodi, kakšna je finančna ocena vira, itd.).
- Vpogled v nabor ocen tveganj
    - Po izbiri posameznega modula dobi uporabnik možnost nove izbire oziroma obstoječe ocene tveganja, ki jo bo uporabljal.
- Izbira posamezne ocene tveganja
    - Po izbiri posamezne ocene tveganja se odpre pregled celotne ocene tveganja ter orodnih vrstic, ki jih ima na voljo uporabnik glede na vlogo. Orodne vrstice morajo biti sestavljene iz polj za urejanje ocene tveganja, pregleda ocene tveganja, pregleda ukrepov in stanja ukrepov.
- Izbiro posameznega dela ocene tveganja (glede na vlogo uporabnika)
    - Glede na vlogo se uporabniku odpre samo del, za katerega je zadolžen (posamezen proces, oddelek), kjer je na voljo ustrezna orodna vrstica.
- Izračun ocene tveganja za posamezne vire oziroma značilnosti delovanja organizacije (izbira posameznih elementov v oceni oziroma, če ni možna izbira, vpisovanje podatkov).

    - Ko uporabnik izbere urejanje ocene tveganja, lahko začne z oceno, ki mu omogoča za vsako tveganje predpripravljene elemente oziroma rešitve, vendar še vedno ostaja možnost dodajanja oziroma vpisovanja lastnih elementov.

- Izračun povprečne ocene tveganja in primerjava med posameznimi ocenami tveganj
    - Za posamezno oceno tveganja se mora izračunati povprečna stopnja tveganja vseh izračunanih tveganj ter to stopnjo primerjati med posameznimi ocenami tveganj (npr. za leto 1 je stopnja 4,36, za leto 2 pa 4,11 – skupna tveganja so zmanjšana za n%)
- Pripravo ukrepov za zmanjšanje tveganj (izbira posameznih elementov med ukrepi oziroma, če ni možna izbira, vpisovanje podatkov)
    - Na podlagi posameznih nesprejemljivih tveganj (po izbrani metodologiji), se morajo uporabniku avtomatsko odpreti polja za ukrepe, ki so lahko že predpripravljeni (iz nabora) oziroma jih uporabnik vpiše sam. Za ukrepe se mora odpirati polje ob samem tveganju, da je povezava čim bolj pregledna. Vpis ukrepa v posamezni oceni tveganja se mora pojaviti v naboru predpripravljenih ukrepov, če ga že ni predhodno vpisal.
- Pregled vseh ukrepov za zmanjšanje tveganj (glede na vlogo uporabnika)
    - Ukrepi se po končani oceni tveganja zberejo v tabeli, ki je dosegljiva uporabniku glede na vlogo. Iz tabele mora biti razvidno, kateri ukrepi so najpomembnejši in kakšen je strošek investicije ter prihranek ob upoštevanju uresničitve tveganja.
- Povezovanje ukrepov med ocenami tveganj
    - Vsi izbrani ukrepi v posameznih ocenah tveganja se morajo povezovati med seboj z namenom natančnega izračuna investicij (en ukrep lahko pokrije več tveganj). Povezovanje mora biti razvidno iz preglednic, ki jih s pomočjo orodja lahko dobi vodstvo, nadzorniki in revizorji.
- Določanje odgovornih oseb za tveganja (glede na vlogo uporabnika)
    - Vsako tveganje se mora določiti posameznim odgovornim osebam (privzeto bi to veljalo za lastnike procesov/vodje oddelkov za njihove procese/oddelke).
- Opozarjanje pooblaščenih oseb na stanja ukrepa (v čakanju, izvedeno, itd.)
    - Vsak ukrep se da v obravnavo posamezni pooblaščeni osebi, ki je dolžna skrbeti za implementacijo. Pred izvedbo ukrepa mora le-ta biti potrjen s strani vodstva, varnostnega inženirja/skrbnikov sistemov vodenja ali lastnikov procesov/vodij (izbira v administrativnem modulu).
- Opozarjanje pooblaščenih oseb na stalne oziroma ponavljajoče ukrepe
    - Vsak ukrep ima določen rok izvedbe ali ponavljajoče termine, pred katerimi se opozarja pooblaščene osebe (14 dni, 7 dni, 3 dni pred izvedbo).
- Opozarjanje odgovornih oseb za tveganja glede izvedbe posameznih ukrepov
    - Vsak izveden ukrep opozori pooblaščeno osebo.
- Opozarjanje varnostnega inženirja oziroma skrbnikov sistemov vodenja o izvedbi ukrepov
    - Vsak izveden ukrep opozori vodstvo, varnostnega inženirja/skrbnike sistemov vodenja ali lastnike procesov/vodje oddelkov.
    - Vsak prekoračen čas ukrepa opozarja vodstvo, varnostnega inženirja/skrbnike sistemov vodenja ali lastnike procesov/vodje oddelkov.
- Pregled stanja izvedenih ukrepov in zmanjšanja tveganj (glede na vlogo uporabnika)

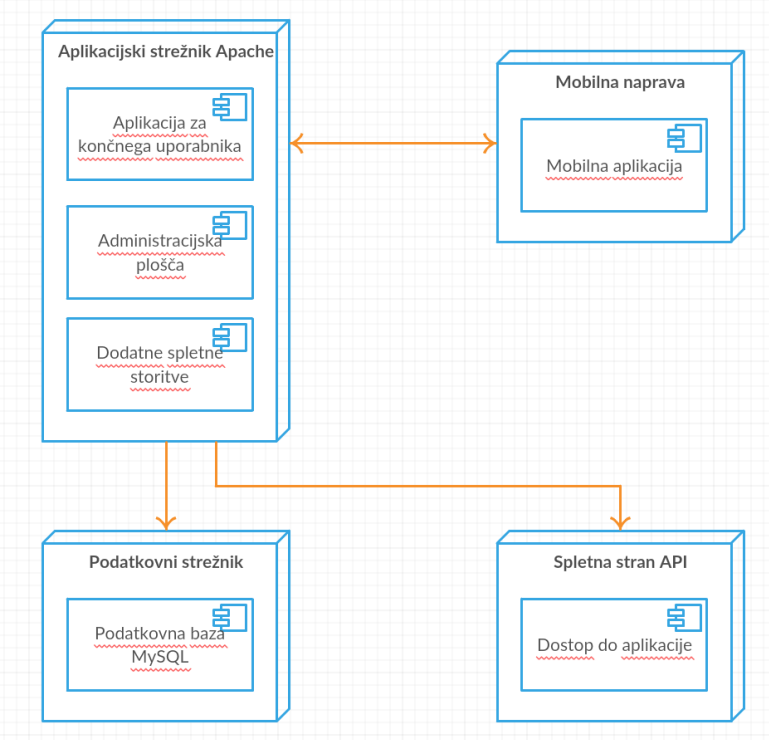
- Ukrepi se po končani oceni tveganja zberejo v tabeli, ki je dosegljiva uporabniku glede na vlogo. Iz tabele mora biti razvidno, kdaj je bil izveden posamezen ukrep oziroma, ali je bil prekoračen dogovorjen čas izvedbe.

- Povezovanje ocen tveganj med seboj in primerjave rezultatov
  - Posamezno oceno tveganja je možno primerjati s prejšnjo oziroma poljubno oceno tveganja iz istega modula. Pri primerjavi je potrebno prikazati, ali so bila tveganja ustrezno zmanjšana.
- Izpis ocene tveganj v standardnih formatih in vzorčnih obrazcih
  - Vse prikaze ocene tveganj je možno izpisati kot standardne formate (format .pdf).

6.1.2 Strojni vmesniki

Programska oprema mora delovati neodvisno od strojne opreme organizacije.

6.1.3 Programski vmesniki



Slika 16: Programski vmesniki OTO

6.1.4 Komunikacijski vmesniki

Programsko opremo bo organizacija namestila v svoj informacijski sistem, kar pomeni, da varnost na komunikacijskem nivoju ni ključnega pomena. Programska oprema bo nameščena na strežniški infrastrukturi ali posamezni delovni postaji in uporabniški dostop bo mogoč z uporabo preko spletnega brskalnika.

6.2 Zahteve glede delovanja programske opreme

Delovanje programske opreme je odvisno od:

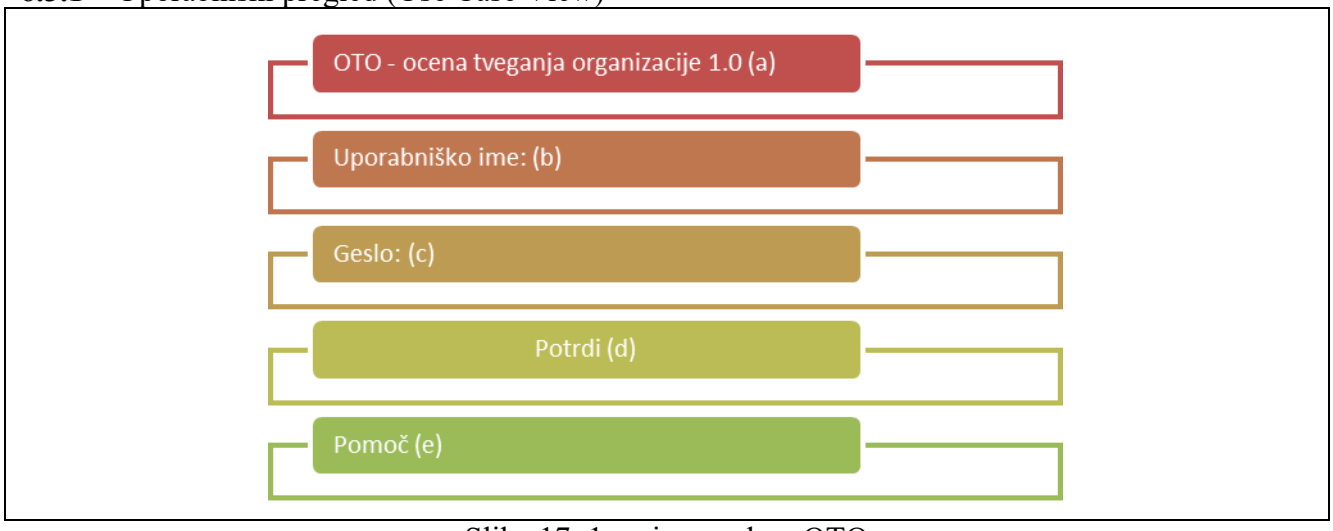
- prijave uporabnika v programsko opremo z enoznačnim uporabniškim imenom (in geslom);
  - To je enako kot pri dostopu do spletno dosegljivih aplikacij, kjer je razviden uporabnik. Programska oprema potrebuje za delovanje dostop do interne mreže.
- vpogleda v nabor modulov;

    - Ta je odvisen od nameščenih modulov. Vpogled je mogoč le v tiste module, ki so dostopni glede na vlogo uporabnika.
- administrativnega modula;
    - To je osnovni modul, ki določa vse ostale module. V administrativnem modulu je možno urejanje in nadgrajevanje programske opreme, zato mora imeti povezavo na splet.
- vpogleda v okolje organizacije (poslovni procesi, organizacijska struktura, viri);
    - Administrator oziroma uporabniki definirajo poslovne procese, organizacijsko strukturo in vire, ki bodo vključeni v obvladovanje tveganj z namenom doseganja ciljev.
- določitve nivoja ocene tveganja (organizacija, posamezna organizacijska enota, poslovni procesi, posamezni viri);
    - Administrator določi, kako se bo izvajala ocena tveganja oziroma, kateri poslovni procesi, organizacijske enote in viri bodo vključeni v posamezni oceni tveganja. Uporabnik dobi možnost vpogleda in dodajanja opisov poslovnih procesov (tudi dodani dokumenti in slike, diagrami), dodajanja opisov organizacijskih enot in virov.
- vpogleda v vire organizacije (značilnosti vira in finančna ocena vira);
    - Uporabniki lahko vidijo vse vire organizacije, ki so pomembni za ocenjevanje tveganj (v katero skupino virov sodi, kakšna je finančna ocena vira).
- vpogleda v nabor ocen tveganj;
    - Po izbiri posameznega modula dobi uporabnik možnost nove oziroma obstoječe izbire ocene tveganja, ki jo bo uporabljal.
- vpogleda v nabor ocen tveganj;
    - Ta je odvisen od izvedenih ocen. Vpogled je možen le v tiste, ki so dostopne glede na vlogo oz. v druge v primeru administratorjevega dostopa.
- izbire posamezne ocene tveganja;
    - Izbira ocene pomeni dostop do podatkov same ocene (npr. ocena tveganja 2014)
- izbire posameznega dela ocene tveganja (glede na vlogo uporabnika);
    - Izbira ocene pomeni dostop do podatkov samega dela ocene glede na vlogo (npr. ocena tveganja 2014 – telekomunikacijske storitve – internetni prenos)
- izračun ocene tveganja za posamezne vire oziroma značilnosti delovanja organizacije (izbira posameznih elementov v oceni oziroma, če ni možna izbira, vpisovanje podatkov);
    - Iskanje po bazi elementov, ki je vezana na posamezno oceno tveganja – verjetnosti grožnj oziroma nevarnosti, nabor sredstev, pomanjkljive kontrole oziroma ranljivosti).
- priprave ukrepov za zmanjšanje tveganj (izbira posameznih elementov med ukrepi oziroma, če ni možna izbira, vpisovanje podatkov);
    - Zadnji del izračuna tveganj je priprava ukrepa, ki se mora vključiti avtomatično, če je prekoračeno sprejemljivo tveganje – izračun iz baze podatkov.
- pregleda vseh ukrepov za zmanjšanje tveganj (glede na vlogo uporabnika);
    - Ukrep se mora povezovati s samo oceno tveganja, tabelo ukrepov ter vlogo posameznega uporabnika.

- povezovanja ukrepov med ocenami tveganj;
    - Ukrepi se morajo povezovati med posameznimi ocenami tveganj (prepoznava ukrepa glede na vpis oziroma nabor podatkov in korelacija med ocenami).
- določanja odgovornih oseb za tveganja (glede na vlogo uporabnika);
    - Ukrep se mora povezovati s samo oceno tveganja, tabelo ukrepov ter vlogo posameznega uporabnika.
- izračuna povprečne ocene tveganja in primerjava med posameznimi ocenami tveganj;
    - Omogočen mora biti izračun in prikaz povprečne vrednosti tveganj ter povezovanje podatkov v bazah in izpis primerjave.
- opozarjanja pooblaščenih oseb za ukrepe glede stanja ukrepa (v čakanju, izvedeno);
    - Ukrep se mora nanašati na samo oceno tveganja, tabelo ukrepov, stanje ukrepa, časa vnosa in rok izvedbe ter obveščanje uporabnikov.
- opozarjanja pooblaščenih oseb na stalne oziroma ponavljajoče ukrepe;
- opozarjanja odgovornih oseb za tveganja glede izvedbe posameznih ukrepov;
- opozarjanja varnostnega inženirja oziroma skrbnikov sistemov vodenja o izvedbi ukrepov;
- pregleda stanja izvedenih ukrepov in zmanjšanih tveganj (glede na vlogo uporabnika);
- povezovanja ocen tveganja med seboj in primerjave rezultatov;
- izpisa ocene tveganj v standardnih formatih in vzorčnih obrazcih.
    - Pripravljen mora biti izpis iz baze v format .pdf.

6.3 Zahteve glede načina delovanja programske opreme (Behaviour Requirements)

6.3.1 Uporabniški pregled (Use Case View)



Slika 17: 1. pojavno okno OTO

(a) Ime aplikacije in verzija – polje se povezuje na verzijo aplikacije

(b) Vpis uporabniškega gesla – polje se povezuje na seznam uporabnikov aplikacije. V kolikor uporabniškega imena ni na seznamu, mora javiti opozorilo (npr. Uporabniško ime ni pravilno.). V kolikor uporabnik pozabi vpisati uporabniško ime, mora javiti opozorilo (npr. Uporabniško ime ni vpisano). Aplikacija mora imeti generično prvo uporabniško ime za administratorja (npr. Administrator) .

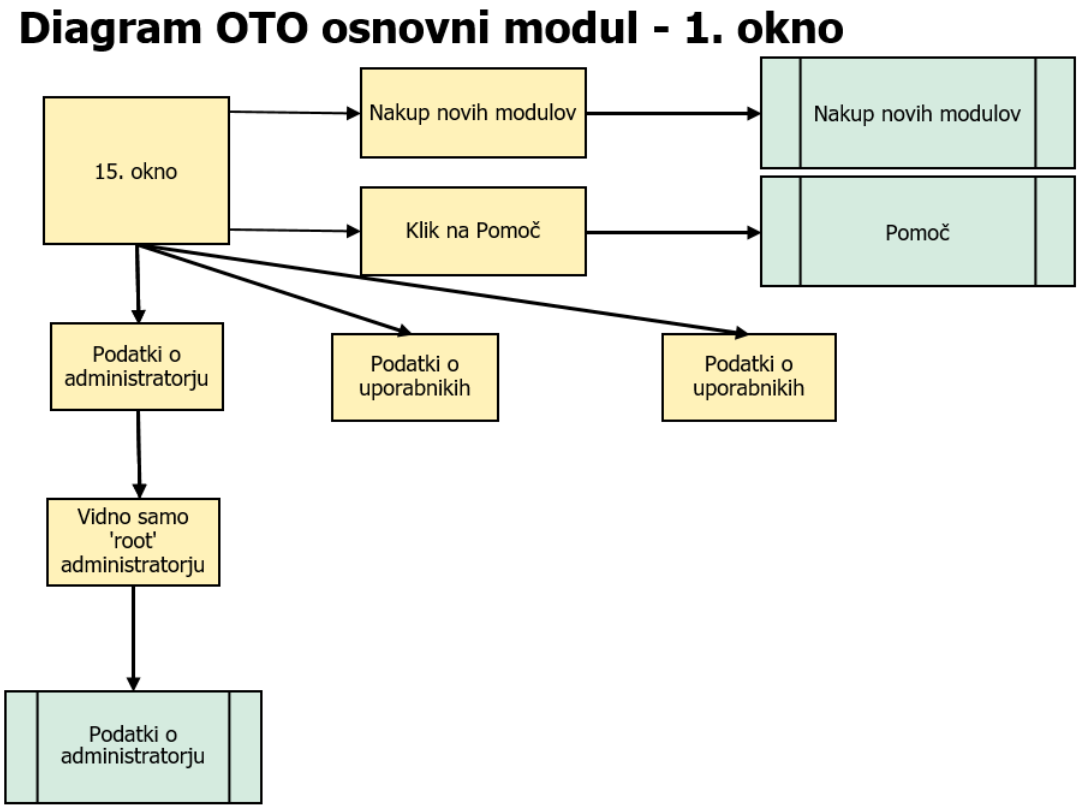
(c) Vpis gesla – polje se povezuje na seznam uporabnikov aplikacije. V kolikor gesla ni na seznamu, mora javiti opozorilo (npr. Geslo ni pravilno). V kolikor uporabnik pozabi vpisati geslo, mora javiti

opozorilo (npr. Geslo ni vpisano.). Aplikacija mora ob prvem zagonu avtomatično določiti geslo za administratorja, ki ga sporoči med samo nastavitvijo aplikacije ali po elektronski pošti.

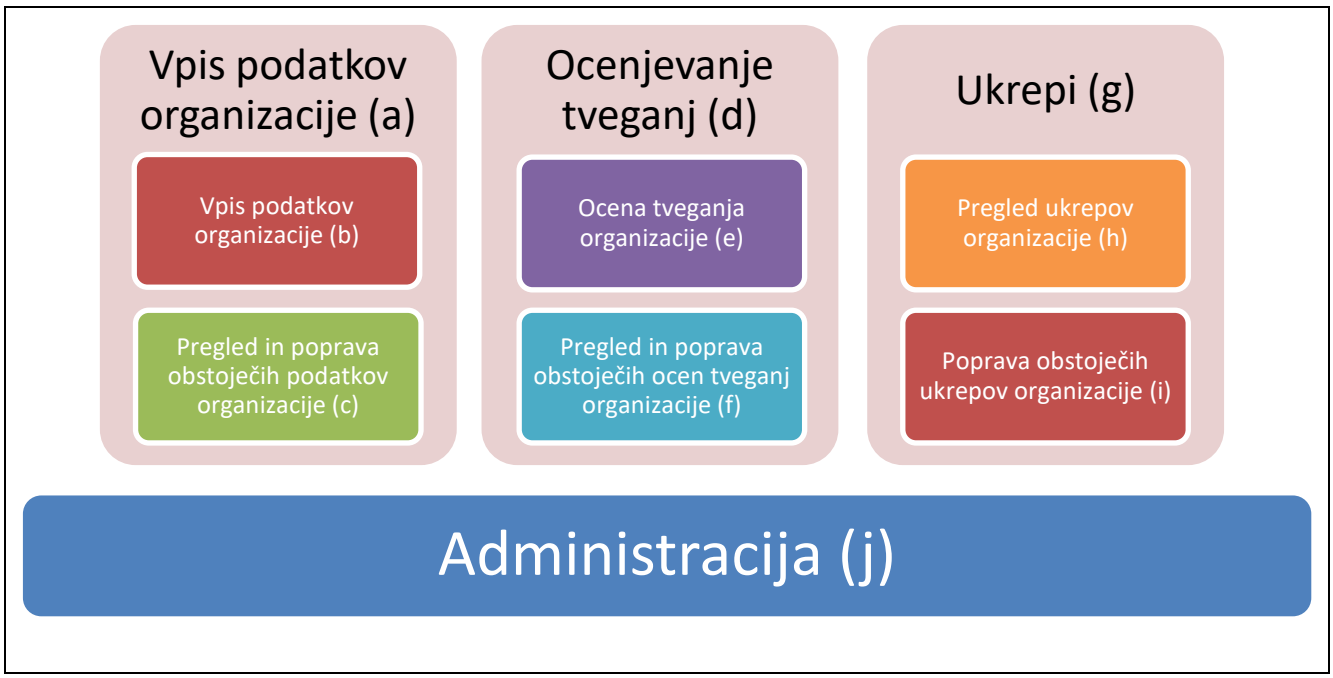
(d) Potrditev uporabniškega imena in gesla oziroma vstop v aplikacijo – ob kliku na gumb potrdi vstop v aplikacijo (pravilna avtentikacija), ali pa se pojavi eden od zgoraj navedenih opozoril (nepravilni ali pomanjkljivi vnos uporabniškega imena in gesla). Po več kot 4 zaporednih napakah, se mora pojaviti opozorilo, da lahko uporabnik zahteva pomoč (oziroma se obrne na vzdrževalca aplikacije – elektronski poštni naslov oziroma avtomatsko sporočilo).

(e) Pomoč uporabniku – opis aplikacije, ki razloži, čemu (ali komu) je aplikacija namenjena (statično besedilo), kontaktni podatki vzdrževalca oziroma polje za avtomatsko posredovanje vprašanj na elektronsko pošto (za morebitno pomoč) in opis značilnosti posamezne verzije (vezano na seznam vsake verzije).

(f) Ozadje – ozadje je narejeno s statično sliko (npr. fotografijo), ki bo opredeljevala risk management in pasico, kjer bi morala biti dinamična vsebina (novi moduli, ki jih ponujamo, obvestila in povezava na spletno stran, kjer lahko stranka kupi nove module oziroma dobi informacije o aplikaciji).



Slika 18: 1. diagram aktivnosti OTO



Slika 19: 2. pojavno okno OTO

(a) Vpis podatkov organizacije – vpis je možen kadarkoli, tudi če ni nobenega modula ocene tveganja.

(b) Nov vpis podatkov organizacije – uporabnika postavi na stran, kjer še ni nobenih podatkov o organizaciji. Funkcija je vedno enaka, ne glede na to, ali je organizacija že vpisana ali ne.

(c) Pregled in poprava obstoječih podatkov – možno, samo če so že vpisani podatki. V kolikor jih ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora opozoriti uporabnika (npr. podatki organizacije še niso vneseni, ko klikne na polje).

(d) Ocenjevanje tveganj – ocenjevanje je možno, če so že vpisani podatki organizacije.

(e) Nova ocena – je možna, samo če so že vpisani podatki organizacije. V kolikor jih ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora uporabnika opozoriti (npr. podatki organizacije še niso vnešeni, ko klikne na polje).

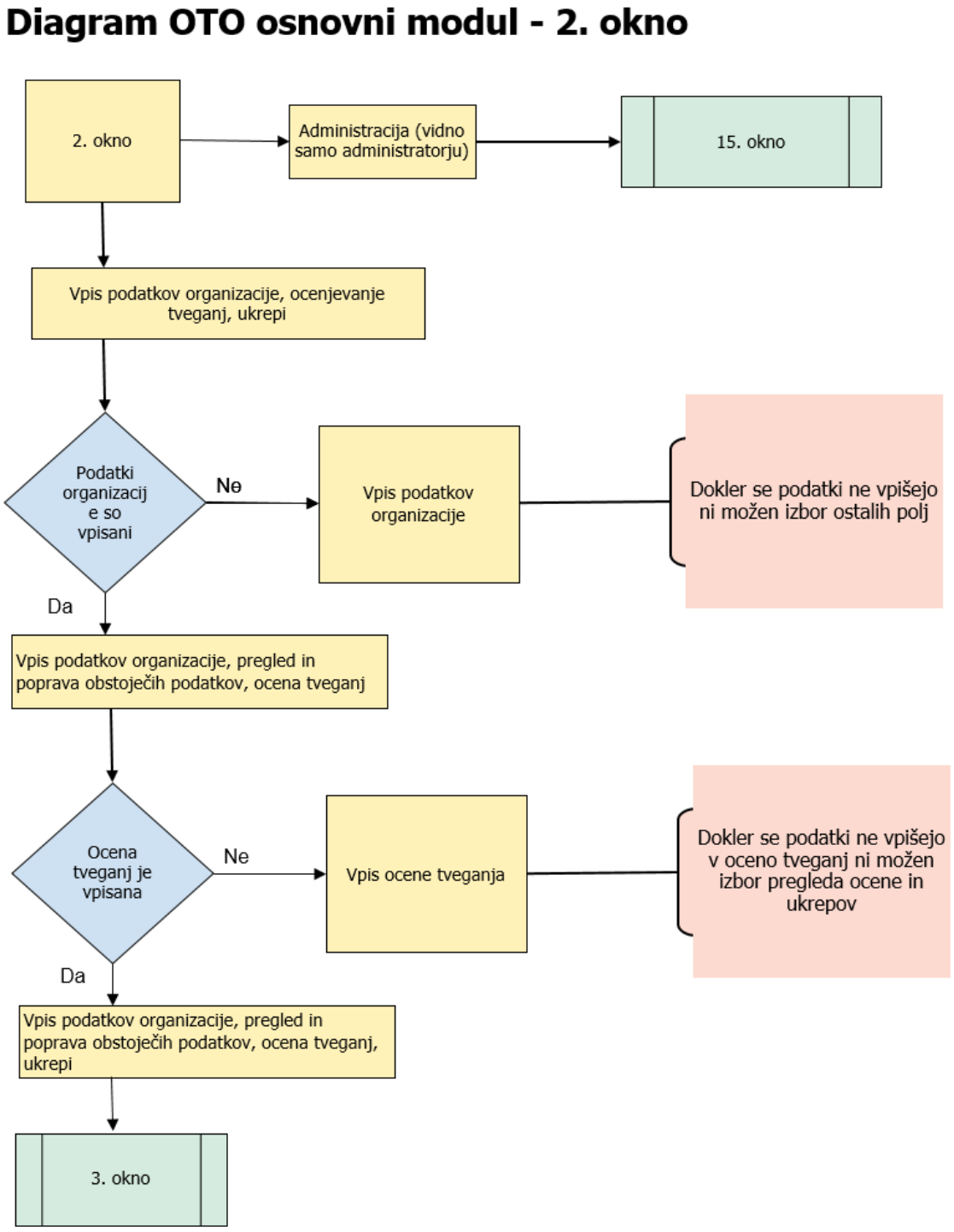
(f) Pregled in poprava ocen – sta možni, samo če so že vpisani podatki organizacije in če je že izvedena ocena tveganja. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora opozoriti uporabnika (npr. podatki organizacije še niso vnešeni, ko klikne na polje oziroma ocena tveganja še ni izvedena).

(g) Ukrepi – pregled ukrepov je možen, če so že vpisani podatki organizacije in izvedena ocena tveganja.

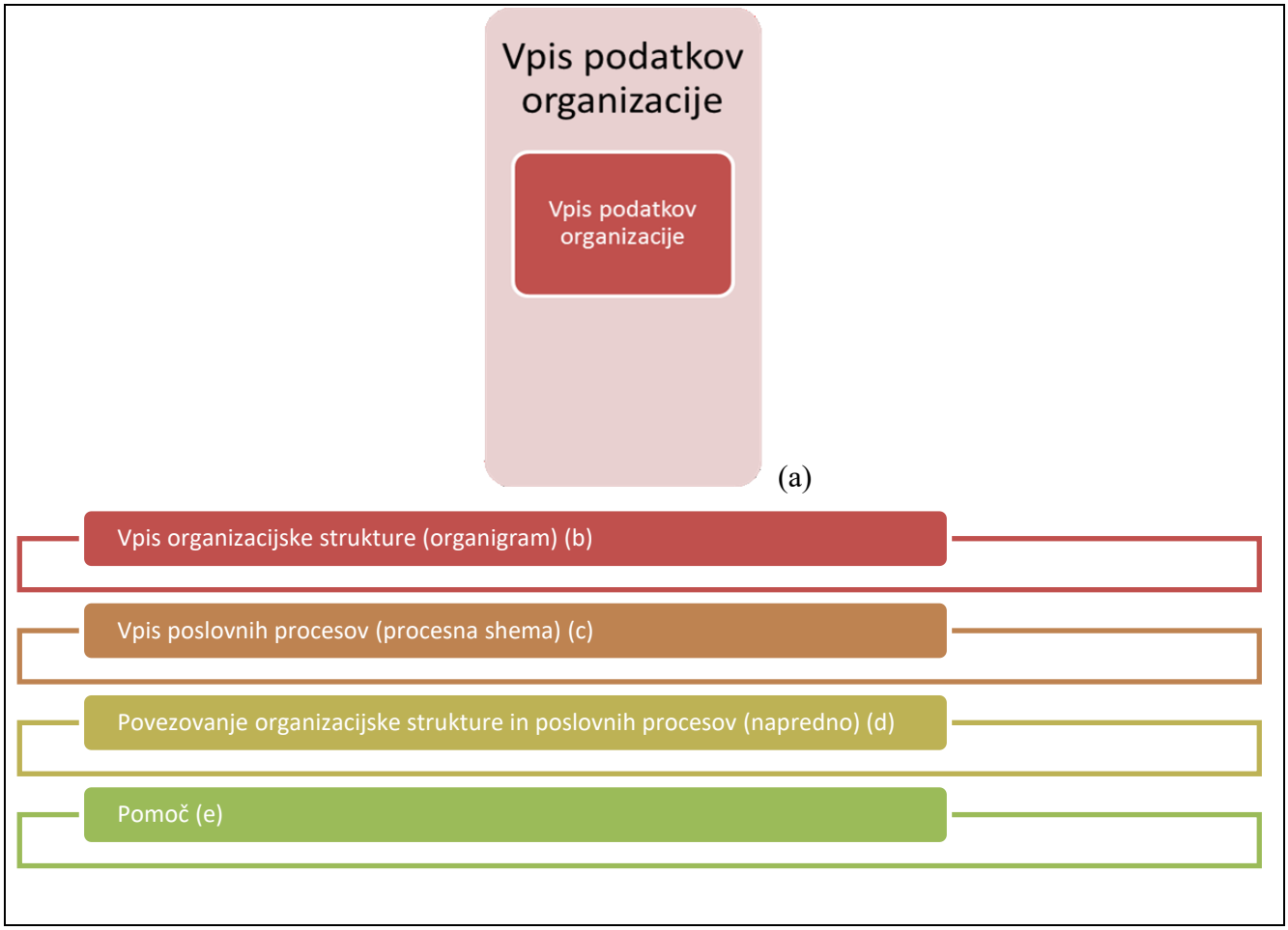
(h) Pregled ukrepov organizacije – je možen, samo če so že vpisani podatki organizacije in če je že izvedena ocena tveganja. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora uporabnika opozoriti (npr. podatki organizacije še niso vnešeni, ko klikne na polje oziroma ocena tveganja še ni izvedena).

(i) Poprava obstoječih ukrepov organizacije – je možna, samo če so že vpisani podatki organizacije, če je že izvedena ocena tveganja in vpisani ukrepi. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora uporabnika opozoriti (npr. podatki organizacije še niso vnešeni, ko klikne na polje, oziroma ocena tveganja še ni izvedena, ukrepi niso vnešeni).

(j) Administracija – polje mora biti vidno samo administratorjem aplikacije. Administratorji lahko določijo, da posamezni uporabnik lahko izbere samo polje Ocena tveganja organizacije, če aplikacijo uporablja veliko število uporabnikov in bi ostala okna lahko povzročala težave pri uporabi aplikacije. To možnost bo potrebno urediti v aplikaciji (polja obarvana 30 % bolj sivo in aplikacija mora uporabnika opozoriti (npr. možno samo ocenjevanje tveganj)).



Slika 20: 2. diagram aktivnosti OTO



Slika 21: 3. pojavno okno OTO

(a) Vpis podatkov organizacije – klik na polje odpre možnosti vpisov organigrama, procesne sheme in povezovanja organigrama in procesne sheme.

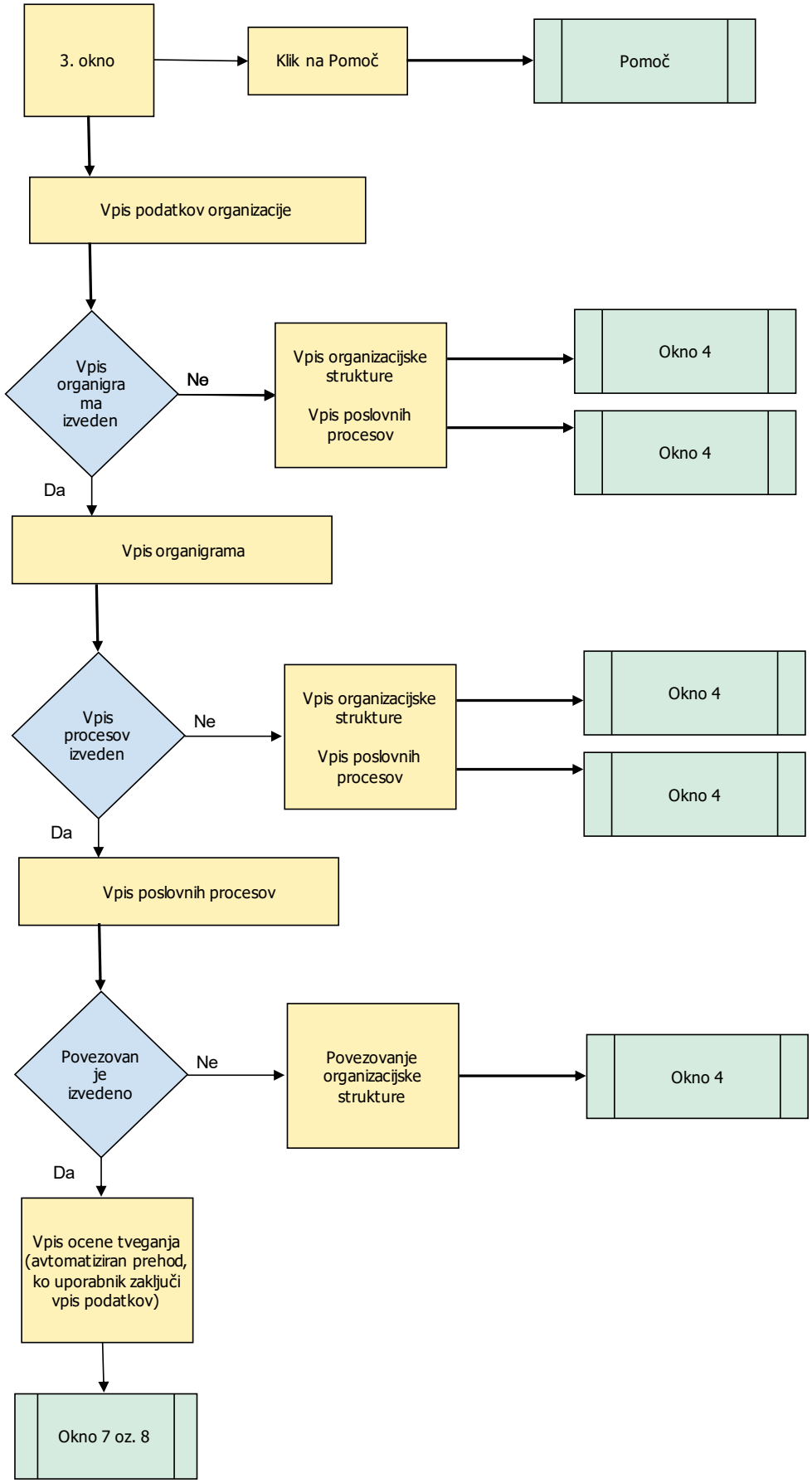
(b) Vpis organizacijske strukture – vpis je nujen za kasnejši vpis procesne sheme in povezovanja.

(c) Vpis poslovnih procesov – je možen, samo če je že vpisan organigram. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora opozoriti uporabnika (npr. organizacijska shema še ni vnešena).

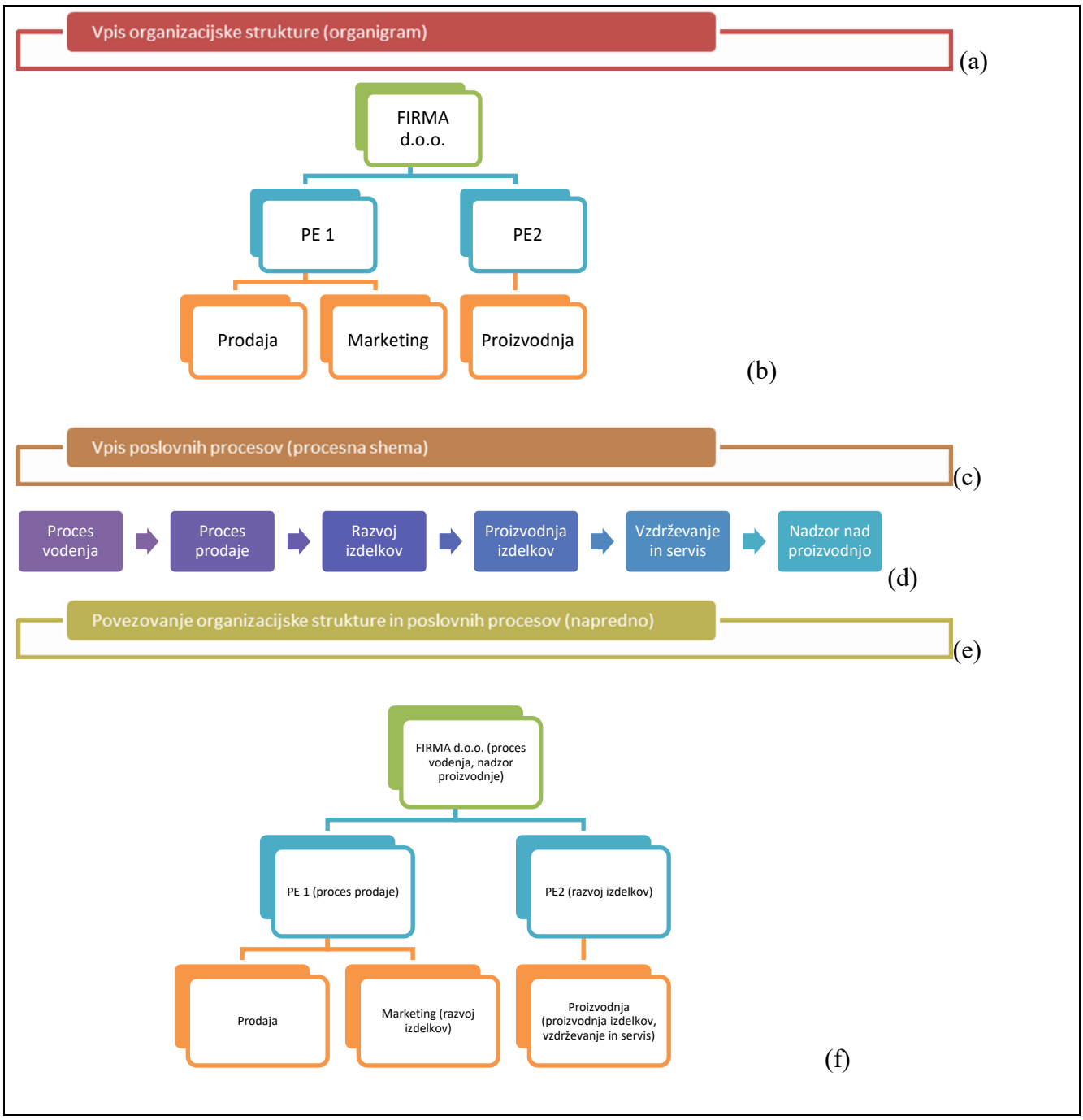
(d) Povezovanje organizacijske strukture in poslovnih procesov – je možno, samo če sta že vpisana organigram in procesna shema. V kolikor nista, mora biti polje obarvano 30 % bolj sivo in aplikacija mora opozoriti uporabnika (npr. organizacijska shema in poslovni procesi še niso vnešeni).

(e) Pomoč – opis, kako mora biti opravljen vpis podatkov, ki razloži, čemu je vpis namenjen (statično besedilo) in slikovno pojasnjeno, na kakšen način se vpisuje.

Diagram OTO osnovni modul - 3. okno



Slika 22: 3. diagram aktivnosti OTO



Slika 23: 4. pojavno okno OTO

(a) Vpis organizacijske strukture – klik na polje odpre okno (b).

(b) Organigram – okno, kjer se odpre polje, kamor se vpiše organizacijska struktura. Organizacijska struktura se začne na vrhu z objektom, ki nima predhodnika (kamor se vpiše organizacijo kot celoto). S tem se lahko organigram lahko zaključi, če ni potrebno vpisati organizacijskih enot oziroma bolj podrobnega opisa organizacije. S tem se ocena tveganja izvaja na celotno organizacijo (OE, delovna sredstva, informacijski sistem, zaposleni, itd.).

Lahko pa se gradi organizacijsko strukturo navzdol, odvisno od potreb organizacije ne glede na število OE oziroma lokacij organizacije. Določitev posameznega nivoja (označeno z različno barvo na sliki (b)) je pomembna, saj se pri ocenjevanju tveganj lahko odloči, na katerem nivoju se bo izvajala ocena tveganja (ta izbira se bo izvajala v posameznem modulu pri ocenjevanju tveganj).

Pokazati se mora povezava med posameznimi objekti (organizacijskimi enotami), kjer je vidno delovanje organizacije. Glede na tip objekta se morajo objekti pokazati v celoti ali delno (npr. tip

objekta OE je vedno viden, tip objekta informacijski sistem pa se lahko skrije, zato da slika ni preveč razdrobljena).

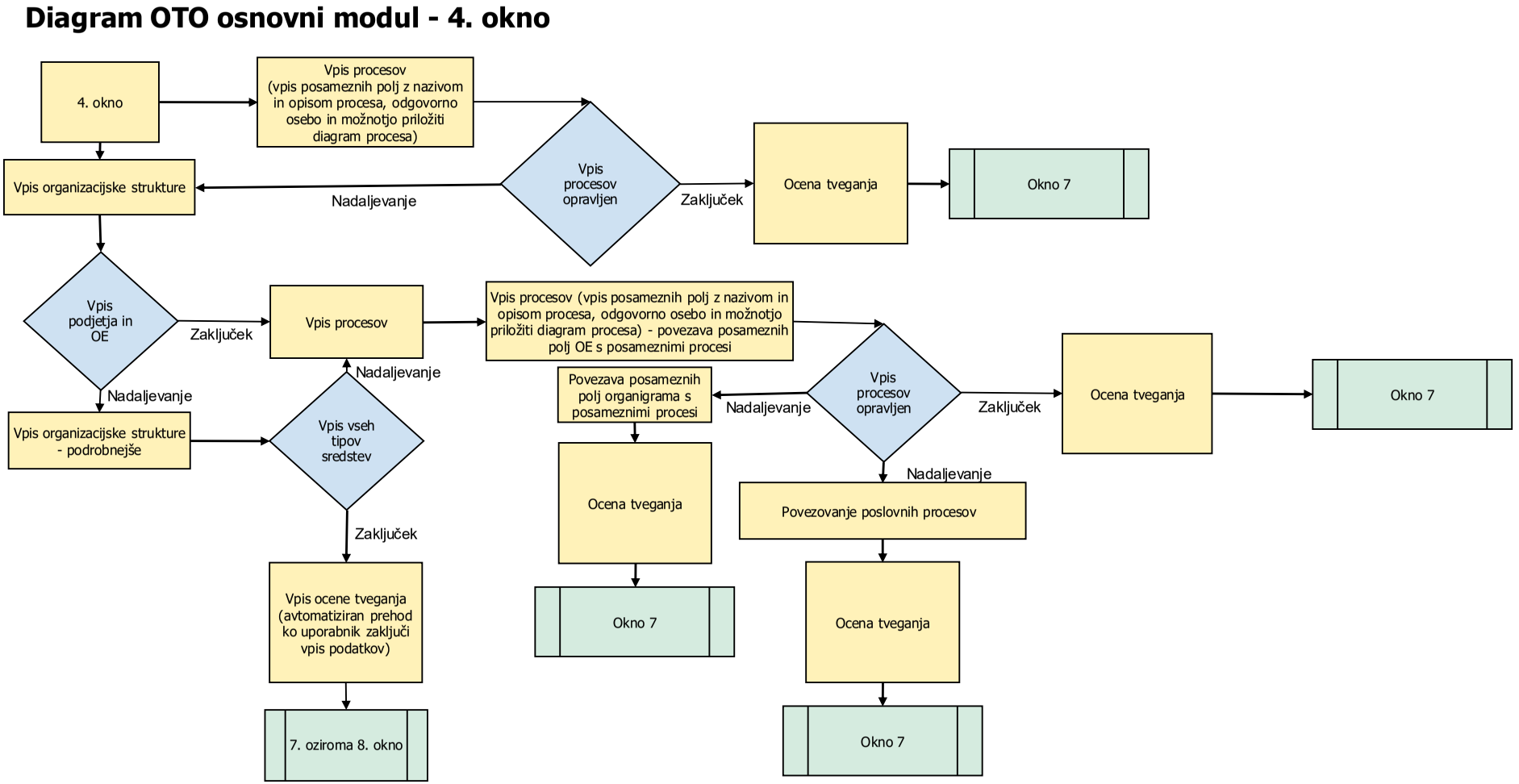
Omogočen mora biti izpis podatkov (format .pdf), da lahko dobi organizacija izpis organigrama (vsi objekti, samo vidni objekti).

(c) Procesna shema – klik na polje odpre okno (d), v kolikor je že izveden organigram. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora uporabnika opozoriti (npr. organizacijska shema še ni vnešena).

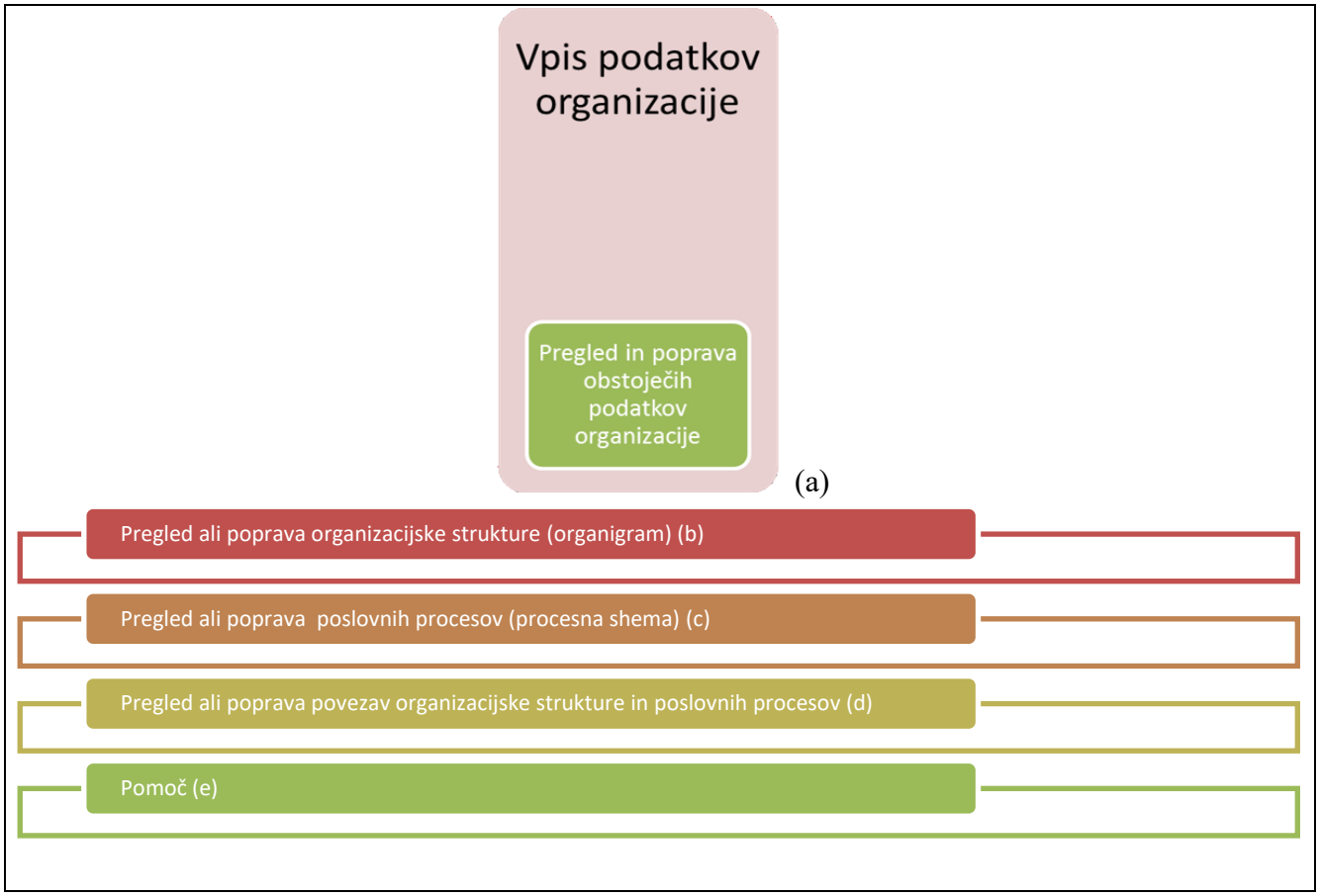
(d) Vpis poslovnih procesov – procese je možno vpisati opisno (npr. proces vodenja). V polje posameznega procesa se lahko doda diagram oziroma opis procesa kot prilogo (sliko, besedilo – zunanjo datoteko, npr. jpg, .doc, itd.). Procese se lahko razdeli v tri skupine (vodstveni, glavni, podporni). Procese se lahko poveže med sabo (posamezen proces sledi drugemu).

(e) Povezovanje organizacijske strukture in poslovnih procesov – klik na polje odpre okno (f), v kolikor sta že izvedena organigram in procesna shema. V kolikor še nista, mora biti polje obarvano 30 % bolj sivo in aplikacija mora opozoriti uporabnika (npr. organizacijska shema in poslovni procesi še niso vnešeni).

(f) Povezovanje (napredno) – odpre se vpisan organigram in za vsak objekt se lahko določi, v kateri poslovni proces spada (smiselno bi bilo, da se procesi različno obarvajo, ali pa se vsak objekt dopolni z opisom procesa (glej sliko (f)), da je takoj razvidno, v kateri poslovni proces spada posamezen objekt (lahko se procese določi po posameznih OE (vidni tipi objektov)) ali pa tudi nižje (poslovni procesi po posameznih delovnih sredstvih, delih informacijskega sistema, delovnih mestih (skriti tipi objektov)).



Slika 24: 4. diagram aktivnosti OTO



Slika 25: 5. pojavno okno OTO

(a) Pregled in poprava obstoječih podatkov organizacije – klik na polje odpre možnost pregleda in poprave organigrama, procesne sheme in povezovanja organigrama in procesne sheme (v kolikor ima uporabnik take pravice). To je možno, samo če je že vpisan organigram. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora opozoriti uporabnika (npr. organigram še ni vnešen).

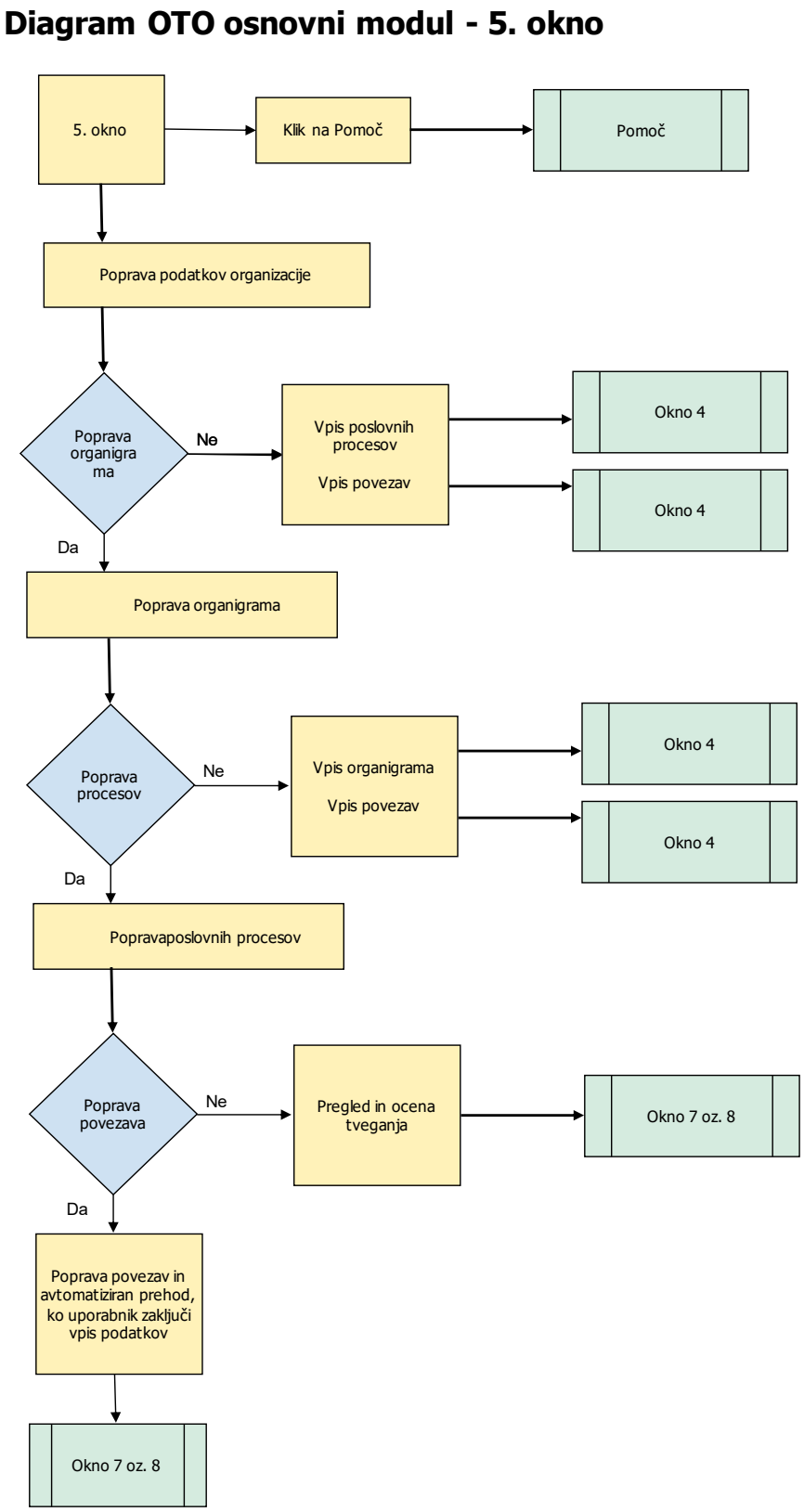
(b) Pregled ali poprava organizacijske strukture – sta možna, samo če je že vpisan organigram. Glej točko (a). V kolikor je bilo vpisanih več organigramov, se mora pojaviti seznam vseh (ID, ime posameznega organigrama, datum vpisa) pred izbiro posameznega, ki ga opravi uporabnik. Seznam mora na dnu polja vsebovati pregled (read-only funkcija), poprava (možnost vnašanja sprememb, če ima uporabnik to pravico) oziroma izbris (če ima uporabnik to pravico).

(c) Pregled ali poprava poslovnih procesov – sta možna, samo če je že vpisana poslovna shema. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora opozoriti uporabnika (npr. procesna shema še ni vnešena). V kolikor je bilo vpisanih več procesnih shem, se mora pojaviti seznam organigramov (ID, ime posameznega organigrama, datum vpisa) in seznam vseh procesnih shem v posameznem organigramu pred izbiro posamezne sheme (ID, ime posamezne procesne sheme, datum vnosa), ki ga opravi uporabnik. Seznam mora na dnu vsebovati polja pregled (read-only funkcija), poprava (možnost vnašanja sprememb, če ima uporabnik to pravico) oziroma izbris (če ima uporabnik to pravico).

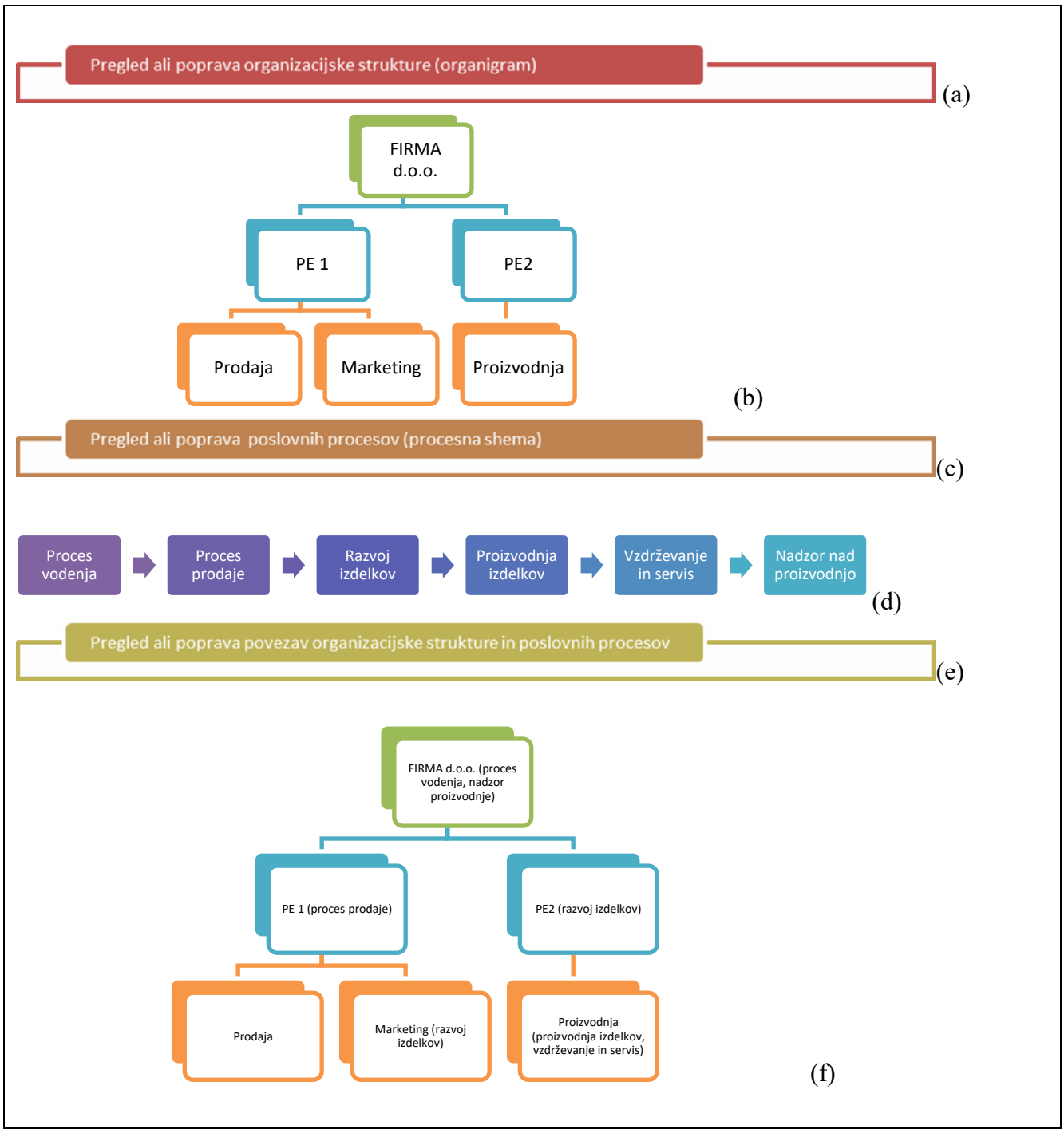
(d) Pregled ali poprava povezav organizacijske strukture in poslovnih procesov – so možni, samo če je že vpisana povezava organigrama in procesna sheme. V kolikor ni, mora biti polje obarvano 30 % bolj sivo in aplikacija mora uporabnika opozoriti (npr. organizacijska shema in poslovni procesi še niso vnešeni). V kolikor je bilo vpisanih več povezav organigramov in procesnih shem, se mora pojaviti seznam organigramov (ID, ime posameznega organigrama, datum vpisa) in seznam vseh povezav procesnih shem in organigramov v posameznem organigramu pred izbiro posamezne povezave (ID, ime posamezne povezave, datum vnosa), ki ga opravi uporabnik. Seznam mora na dnu

vsebovati polja pregled (read-only funkcija), poprava (možnost vnašanja sprememb, če ima uporabnik to pravico) oziroma izbris (če ima uporabnik to pravico).

(e) Pomoč – je opis, kako morata biti opravljena pregled in poprava podatkov, ki razloži, čemu sta pregled in poprava namenjena (statično besedilo) in slikovno pojasnjeno, na kakšen način se lahko pregleduje in popravlja.



Slika 26: 5. diagram aktivnosti OTO



Slika 27: 6. pojavno okno OTO

(a) Pregled in poprava organizacijske strukture – klik na polje odpre okno s seznamom vseh organigramov, ki so bili pripravljeni (ID, ime posameznega organigrama, datum vpisa). Uporabnik posameznega organigrama lahko izbere tistega, ki ga želi. Seznam mora na dnu vsebovati polja pregled (read-only funkcija), poprava (možnost vnašanja sprememb, če ima uporabnik to pravico) oziroma izbris (če ima uporabnik to pravico).

(b) Organigram – okno, kjer se odpre želeni organigram, kakor je bil vpisan. Vidna mora biti povezava med posameznimi objekti (organizacijskimi enotami), ki nam pokaže, kako organizacija deluje. Glede na tip objekta se morajo objekti pokazati v celoti ali deloma (npr. tip objekta OE je vedno viden, tip objekta informacijski sistem pa se lahko skrije, da ni prevelike razdrobljenosti slike).

Omogočen mora biti izpis podatkov (format .pdf), izpis organigrama (vsi objekti, samo vidni objekti).

Organigram se lahko pregleduje ali popravlja glede na pravice uporabnika.

(c) Pregled ali poprava procesne sheme – klik na polje odpre okno s seznamom vseh organigramov (ID, ime posameznega organigrama, datum vpisa) in vseh procesnih shem v posameznem organigramu pred izbiro posamezne sheme (ID, ime posamezne procesne sheme, datum vnosa), ki ga opravi uporabnik. Seznam mora na dnu vsebovati polja pregled (read-only funkcija), poprava (možnost vnašanja sprememb, če ima uporabnik to pravico) oziroma izbris (če ima uporabnik to pravico). V kolikor še ni vpisane procesne sheme, mora biti polje obarvano 30 % bolj sivo in aplikacija mora na to opozoriti uporabnika (npr. organizacijska shema še ni vnešena).

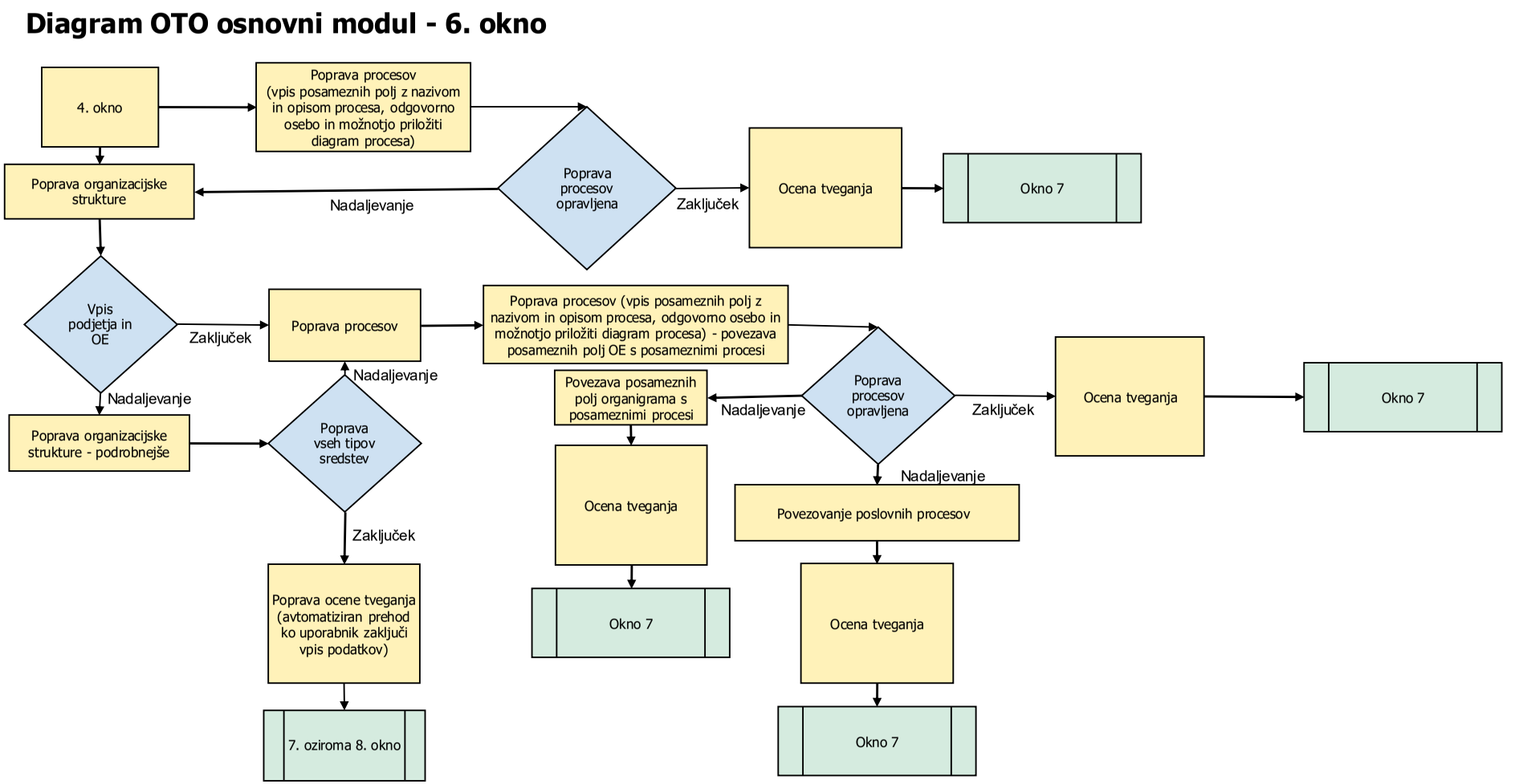
Omogočen mora biti izpis podatkov (format .pdf), da lahko organizacija dobi izpis procesne sheme.

Procesna shema se lahko pregleduje ali popravlja glede na pravice uporabnika.

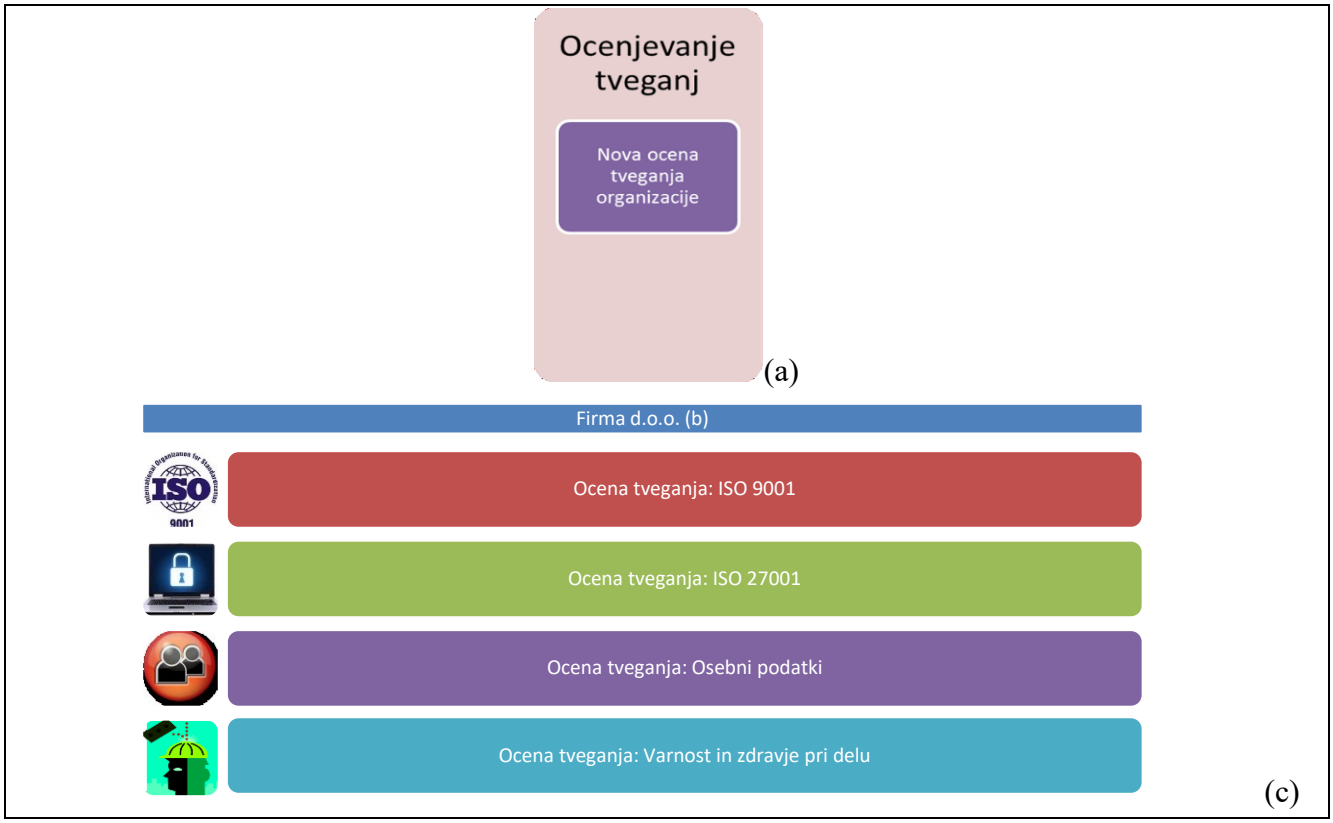
(d) Pregled poslovnih procesov – procese se lahko pregleduje ali popravlja, tako opis procesa kot priloge (slika, besedilo – zunanja datoteka, format .pdf).

(e) Pregled ali poprava povezav organizacijske strukture in poslovnih procesov – klik na polje odpre okno s seznamom vseh organigramov (ID, ime posameznega organigrama, datum vpisa) in vseh povezav v posameznem organigramu pred izbiro posamezne ID, (ime posamezne povezave, datum vnosa), ki ga opravi uporabnik. Seznam mora na dnu vsebovati polja pregled (read-only funkcija), poprava (možnost vnašanja sprememb, če ima uporabnik to pravico) oziroma izbris (če ima uporabnik to pravico). V kolikor še ni vpisane procesne sheme, mora biti polje obarvano 30 % bolj sivo in aplikacija mora na to opozoriti uporabnika (npr. organizacijska shema še ni vnešena, ko klikne na polje).

(f) Povezovanje (napredno) – odpre se želen organigram. Za vsak objekt lahko pregledamo, ali popravimo (glede na pravice uporabnika), v kateri poslovni proces spada (smiselno bi bilo, da se procesi različno obarvajo ali pa se vsak objekt dopolni z opisom procesa (glej sliko (f)), da je takoj vidno, v kateri poslovni proces posamezen objekt spada (lahko se procese določi po posameznih OE (vidni tipi objektov), ali pa tudi nižje (poslovni procesi po posameznih delovnih sredstvih, delih informacijskega sistema, delovnih mestih (skriti tipi objektov)).



Slika 28: 6. diagram aktivnosti OTO

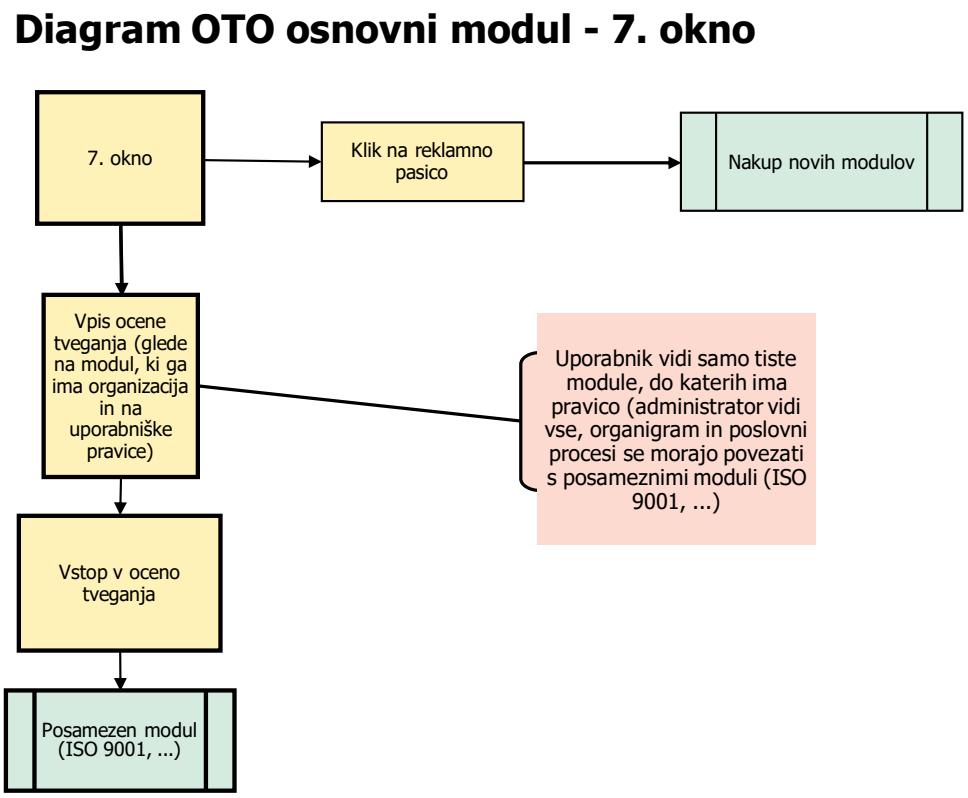


Slika 29: 7. pojavno okno OTO

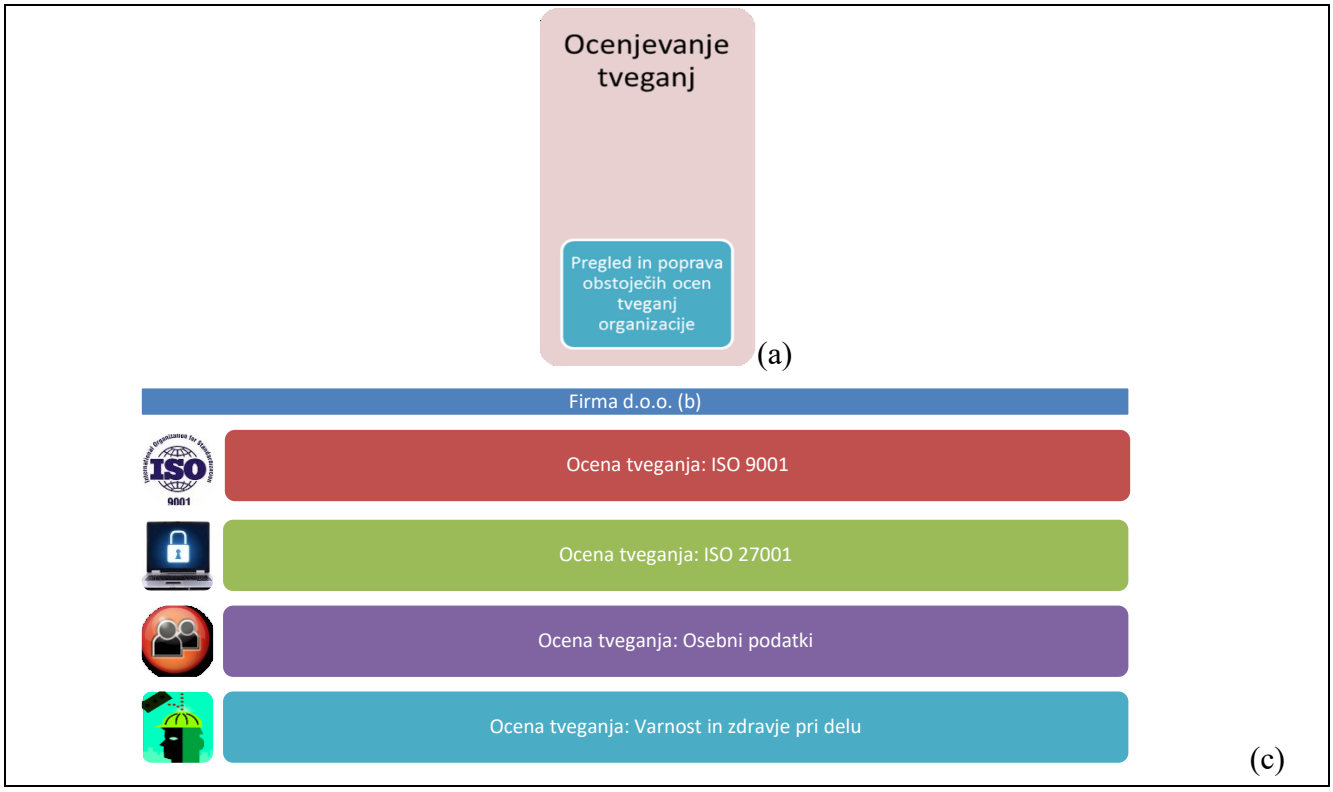
(a) Nova ocena tveganja – klik na polje odpre seznam možnih ocen tveganja, ki jih ima organizacija.

(b) Vpis naziva organizacije – polje se povezuje na prvi objekt pri vpisu podatkov.

(c) Nabor ocen tveganja (modulov), ki jih ima organizacija (vsaj 1 modul) ob nakupu aplikacije.



Slika 30: 7. diagram aktivnosti OTO

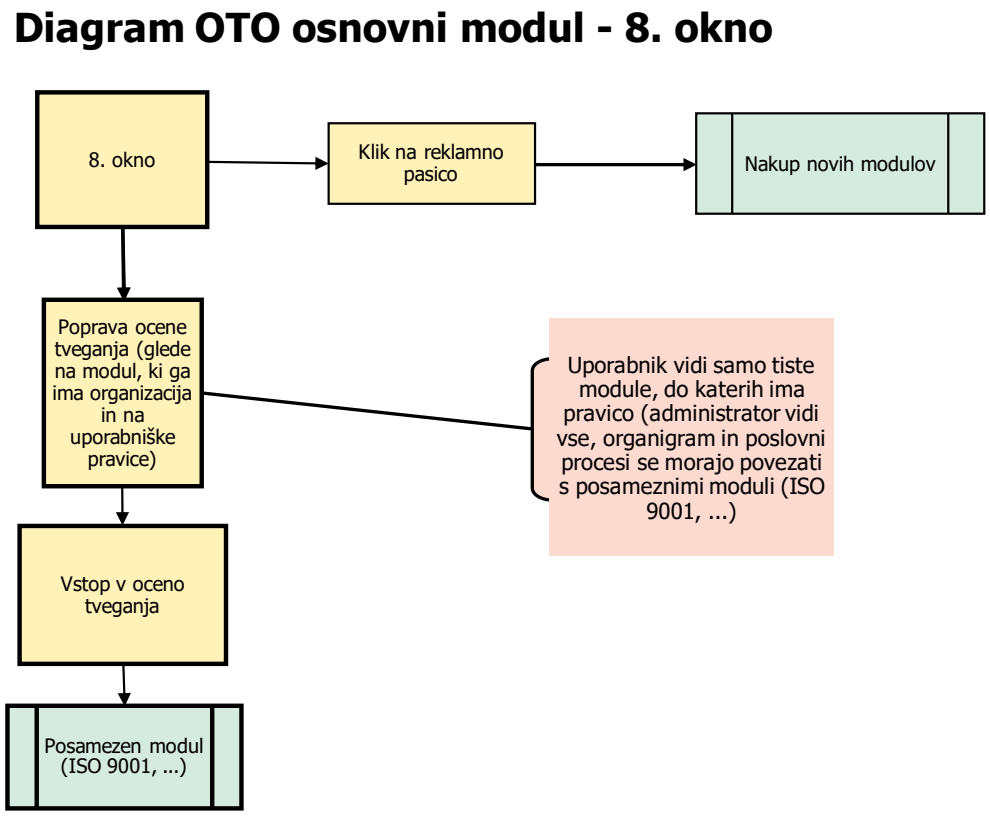


Slika 31: 8. pojavno okno OTO

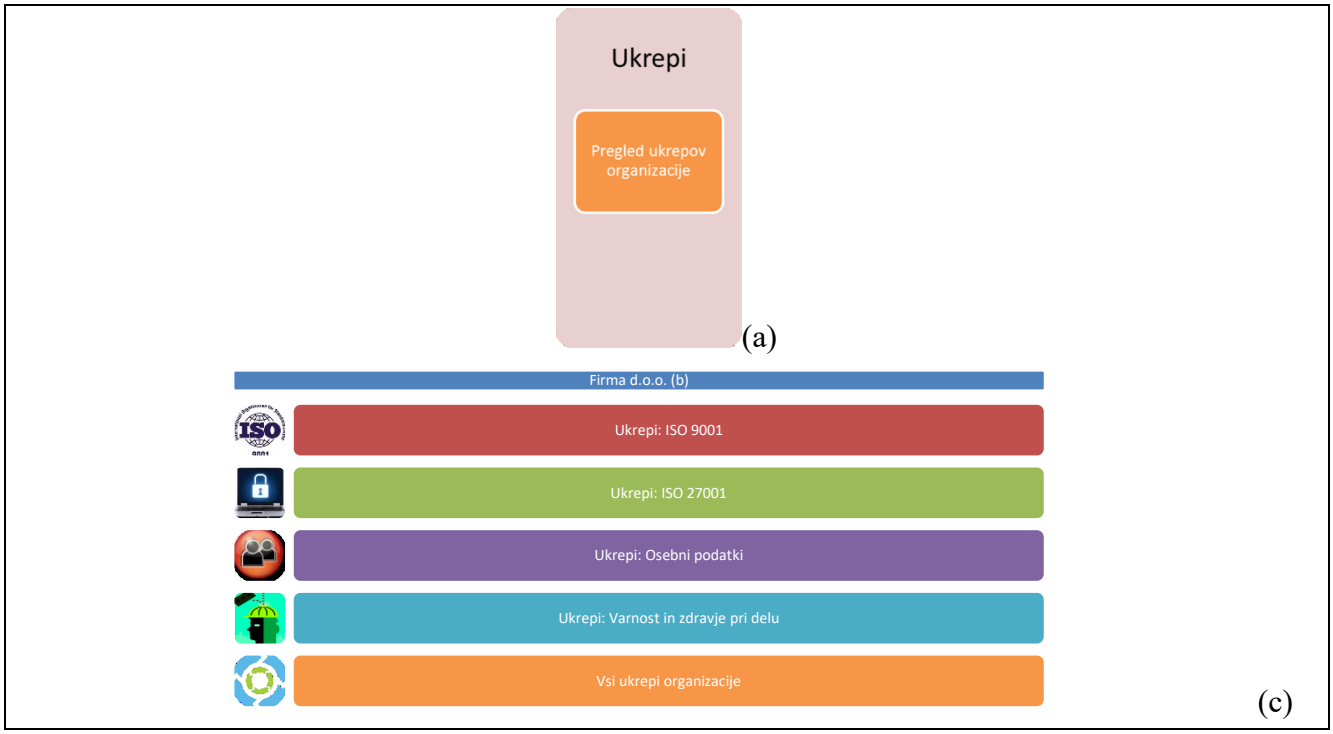
(a) Pregled in poprava ocene tveganja – klik na polje odpre seznam možnih ocen tveganja, ki jih ima organizacija.

(b) Vpis naziva organizacije – polje se povezuje na prvi objekt pri vpisu podatkov.

(c) Nabor ocen tveganja (modulov), ki jih ima organizacija (vsaj 1 modul) ob nakupu aplikacije.



Slika 32: 8. diagram aktivnosti OTO

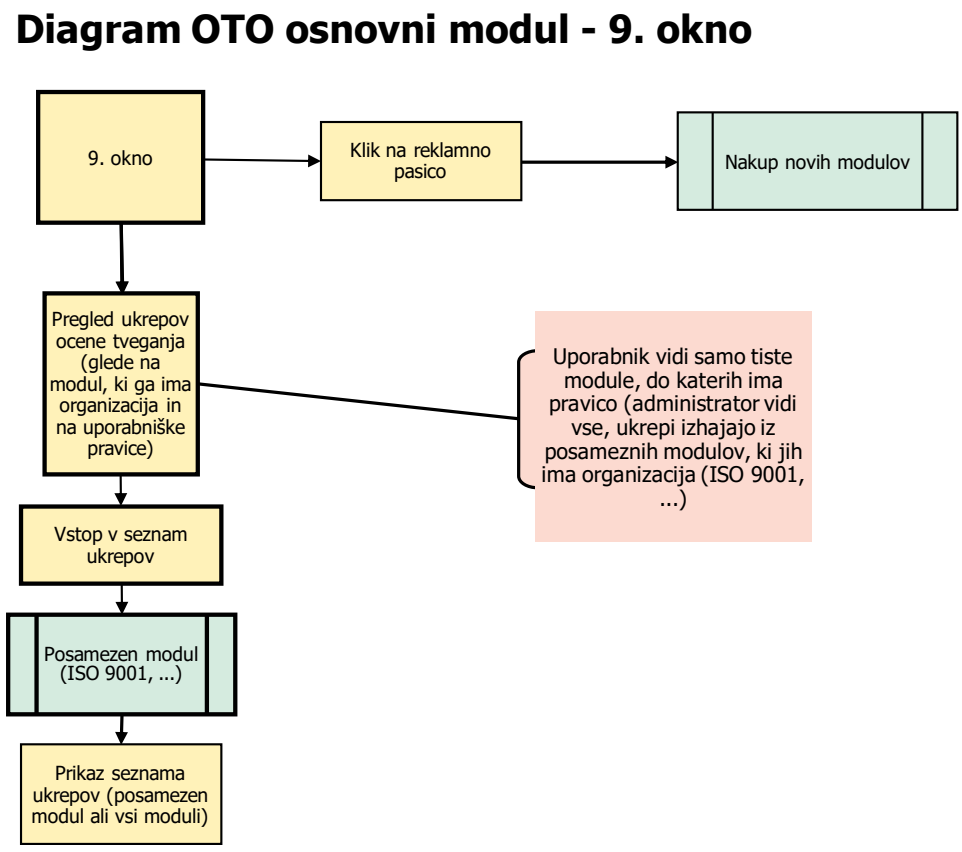


Slika 33: 9. pojavno okno OTO

(a) Pregled ukrepov – klik na polje odpre seznam ukrepov možnih ocen tveganja, ki jih ima organizacija.

(b) Vpis naziva organizacije – polje se povezuje na prvi objekt pri vpisu podatkov.

(c) Nabor ukrepov ocen tveganja (modulov), ki jih ima organizacija (vsaj 1 modul) ob nakupu aplikacije po izvedeni oceni tveganja.



Slika 34: 9. diagram aktivnosti OTO

Slika 35: 10. pojavno okno OTO

(a) Ukrepi: x modul - odpre se tabela ukrepov, kjer so razvidni podatki o vseh ukrepih npr. ISO 9001. Ukrepi se morajo razvrščati glede na posamezen stolpec (npr. stopnja tveganja, rok izvedbe). Nosilec ukrepa je posamezen uporabnik organizacije. Ukrepi so vidni samo nosilcem ukrepov, administratorju ter lastnikom posameznih OE ali poslovnih procesov. Npr:

ID	Ukrep	Stopnja tveganja	Datum vpisa	Nosilec ukrepa	Rok izvedbe	Datum izvedbe (lahko stalni ukrep)	Status	Datum ponovnega pregleda ukrepa (nujno v primeru stalnih ukrepov)

Slika 36: Tabela ukrepov posamezne ocene tveganja OTO

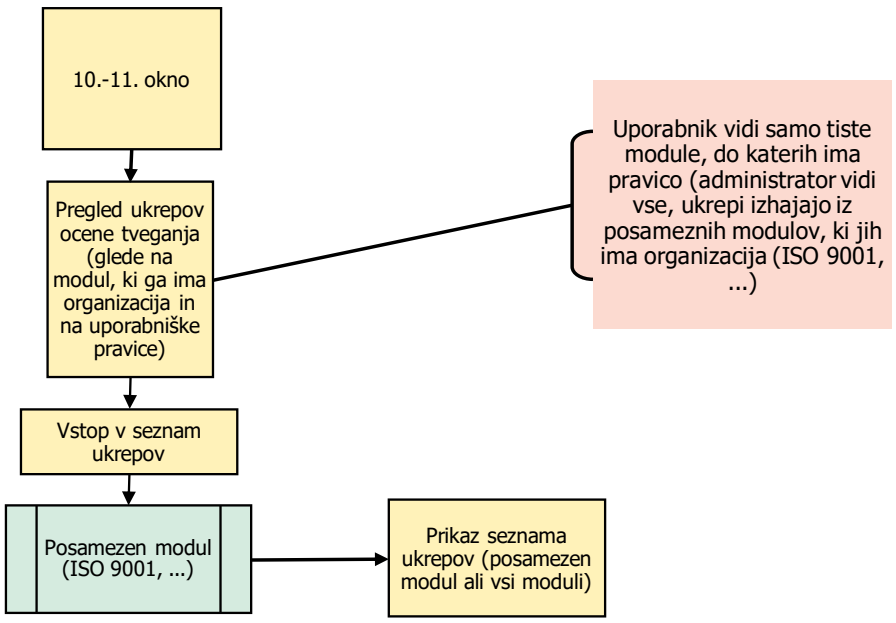
Slika 37: 11. pojavno okno OTO

(a) Ukrepi: vsi moduli - odpre se tabela ukrepov, kjer so razvidni podatki o vseh ukrepih organizacije. Ukrepi se morajo razvrščati glede na posamezen stolpec (npr. stopnja tveganja, rok izvedbe). Nosilec ukrepa je posameznen uporabnik organizacije. Ukrepi so vidni samo nosilcem ukrepov, administratorju ter lastnikom posameznih OE ali poslovnih procesov.

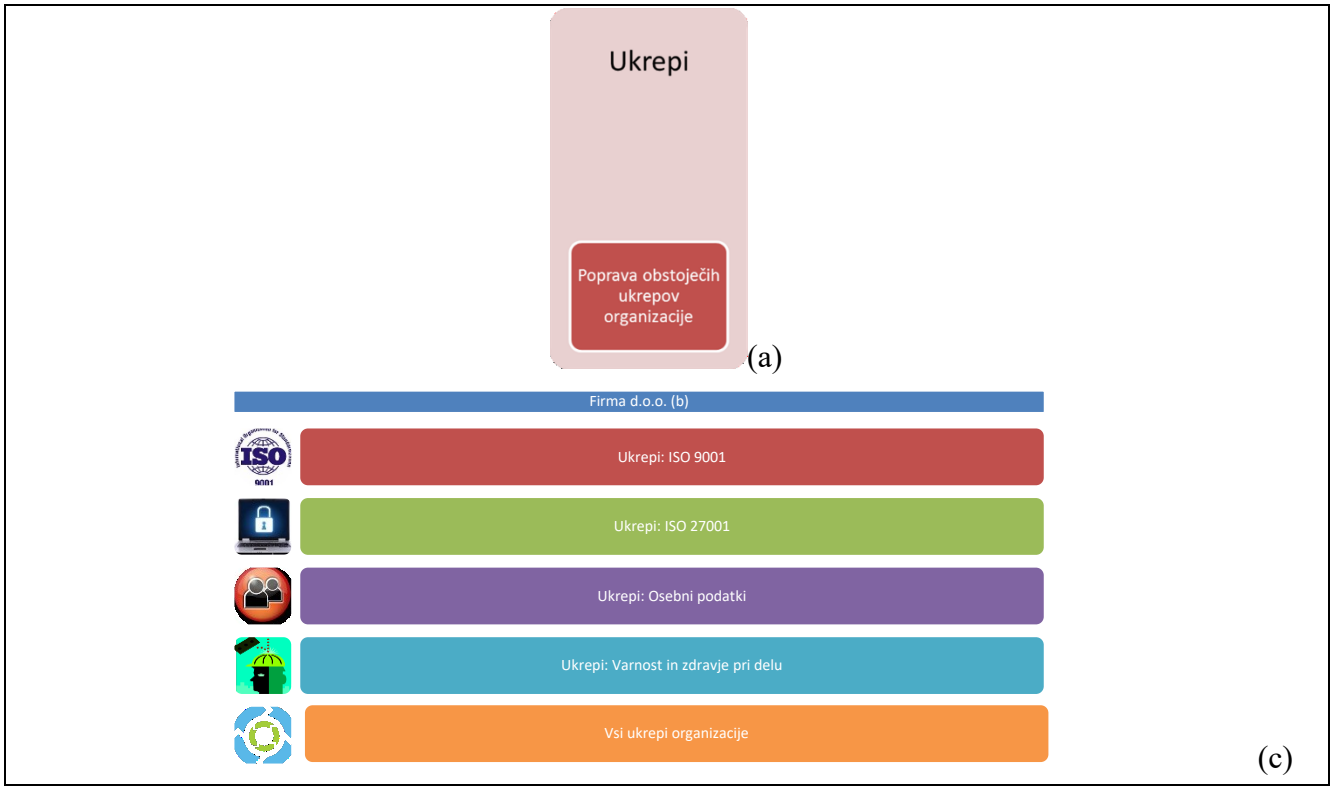
ID	Ukrep	Stopnja tveganja	Datum vpisa	Nosilec ukrepa	Rok izvedbe	Datum izvedbe (lahko stalni ukrep)	Status	Datum ponovnega pregleda ukrepa (nujno v primeru stalnih ukrepov)

Slika 38: Tabela vseh ukrepov OTO

Diagram OTO osnovni modul - 10.-11. okno



Slika 39: 10. in 11. diagram aktivnosti OTO

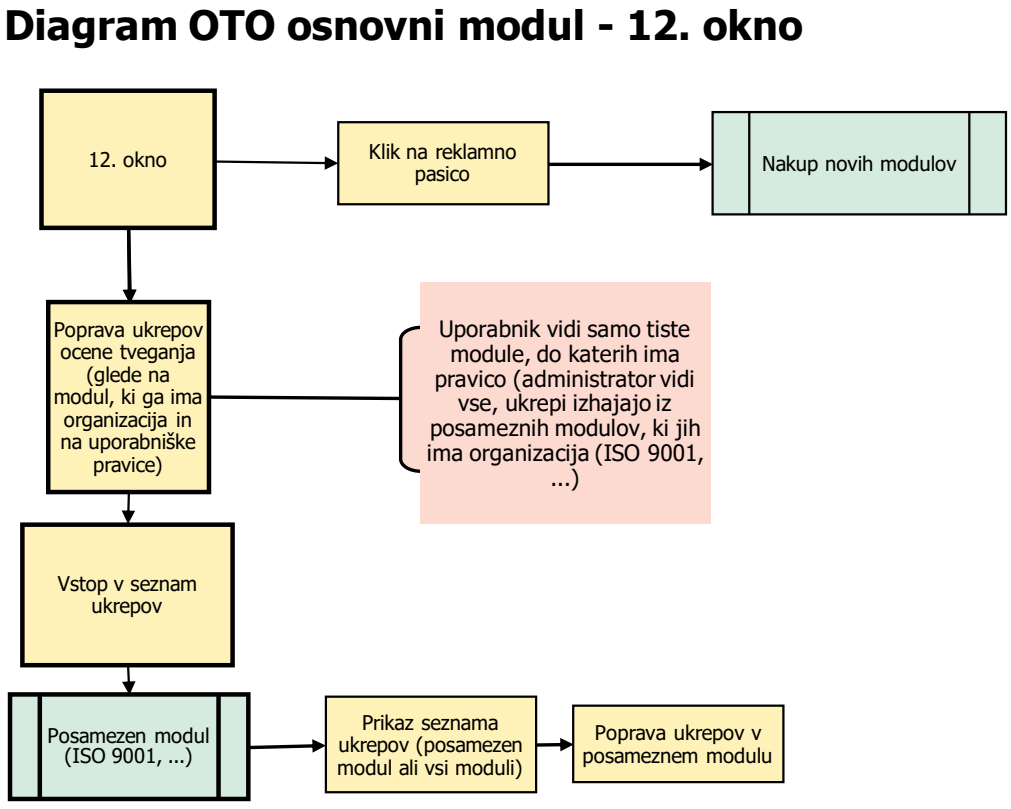


Slika 40: 12. pojavno okno OTO

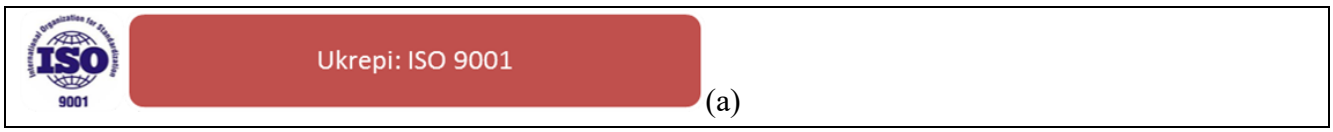
(a) Poprava ukrepov – klik na polje odpre seznam ukrepov možnih ocen tveganja, ki jih ima organizacija.

(b) Vpis naziva organizacije – polje se povezuje na prvi objekt pri vpisu podatkov.

(c) Nabor ukrepov ocen tveganja (modulov), ki jih ima organizacija (vsaj 1 modul) ob nakupu aplikacije po izvedeni oceni tveganja.



Slika 41: 12. diagram aktivnosti OTO



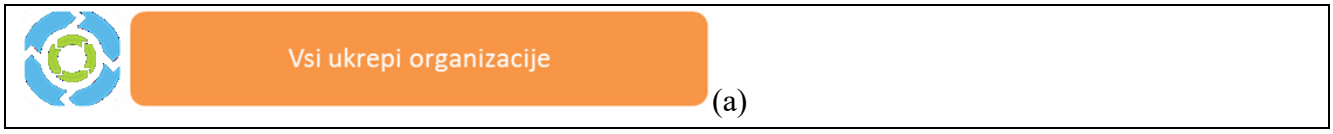
(a)

Slika 42: 13. pojavno okno OTO

(a) Ukrepi: x modul - odpre se tabela ukrepov, kjer so razvidni podatki o vseh ukrepih npr. ISO 9001. Ukrepe lahko popravljajo izključno lastniki poslovnih procesov in OE. Nosilec ukrepa, nadrejeni OE ali lastnik procesa, ki je vključen, so obveščeni o spremembi, ki se beleži tudi v zgodovini sprememb.

ID	Ukrep	Stopnja tveganja	Datum vpisa	Nosilec ukrepa	Rok izvedbe	Datum izvedbe (lahko stalni ukrep)	Status	Datum ponovnega pregleda ukrepa (nujno v primeru stalnih ukrepov)

Slika 43: Tabela ukrepov posamezne ocene tveganja OTO



(a)

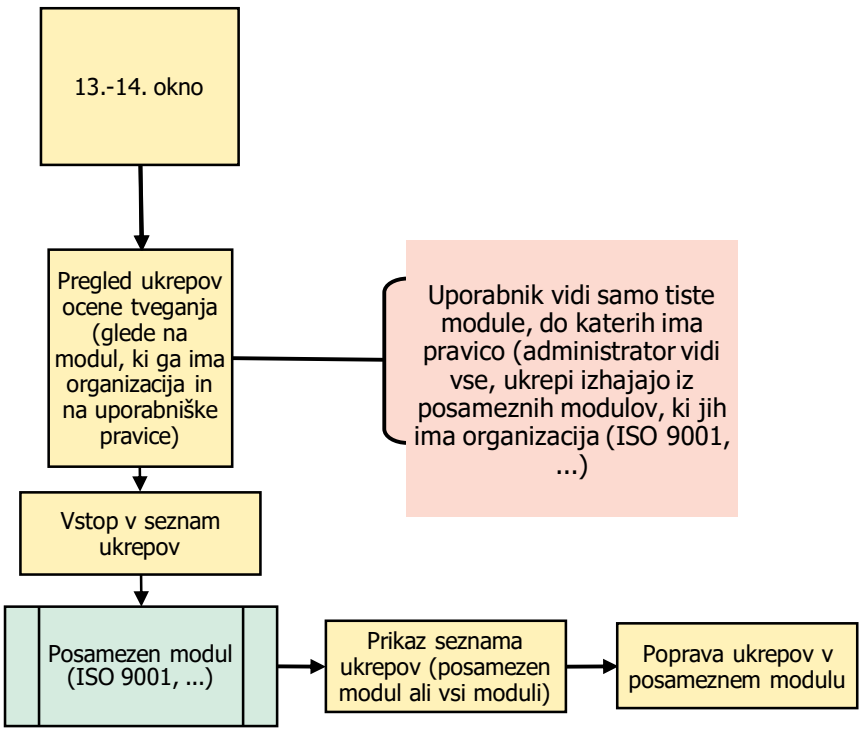
Slika 44: 14. pojavno okno OTO

(a) Ukrepi: vsi moduli - odpre se tabela ukrepov, kjer so razvidni podatki o vseh ukrepih organizacije. Ukrepe lahko popravljajo izključno lastniki poslovnih procesov in OE. Nosilec ukrepa, nadrejeni OE ali lastnik procesa, ki je vključen, so obveščeni o spremembi, ki se beleži tudi v zgodovini sprememb.

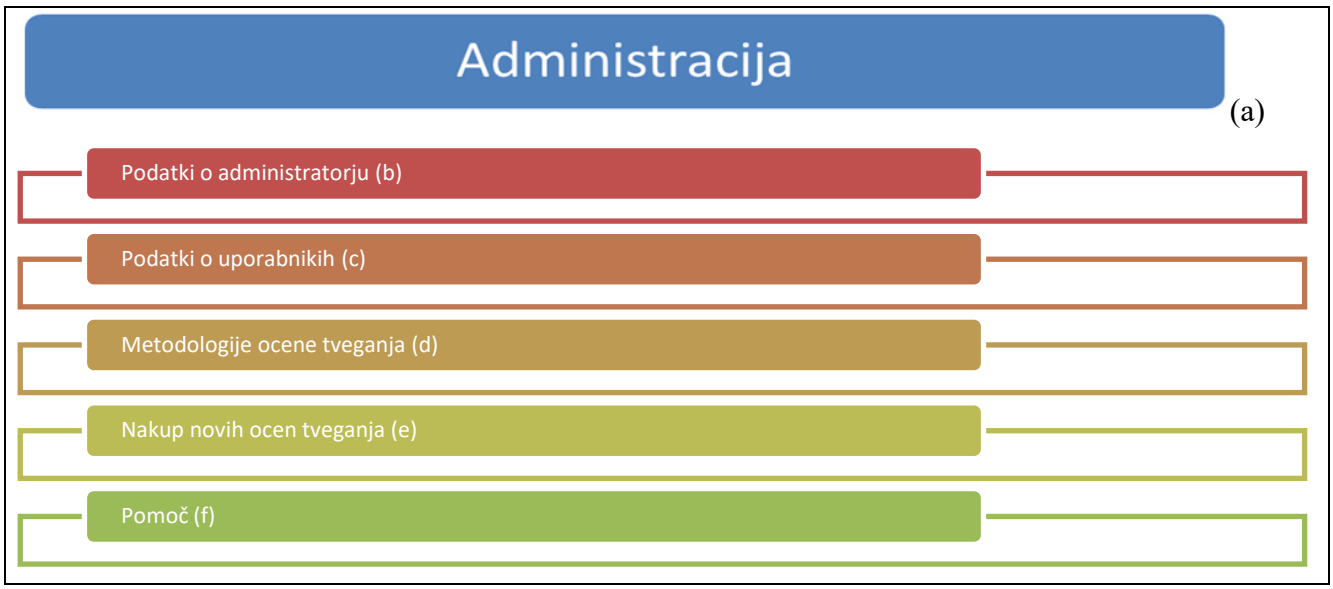
ID	Ukrep	Stopnja tveganja	Datum vpisa	Nosilec ukrepa	Rok izvedbe	Datum izvedbe (lahko stalni ukrep)	Status	Datum ponovnega pregleda ukrepa (nujno v primeru stalnih ukrepov)

Slika 45: Tabela vseh ukrepov OTO

Diagram OTO osnovni modul - 13.-14. okno



Slika 46: 13. in 14. diagram aktivnosti OTO



Slika 47: 15. pojavno okno OTO

(a) Administracija – klik na gumb odpre nabor aktivnosti, ki jih lahko izvaja administrator aplikacije.

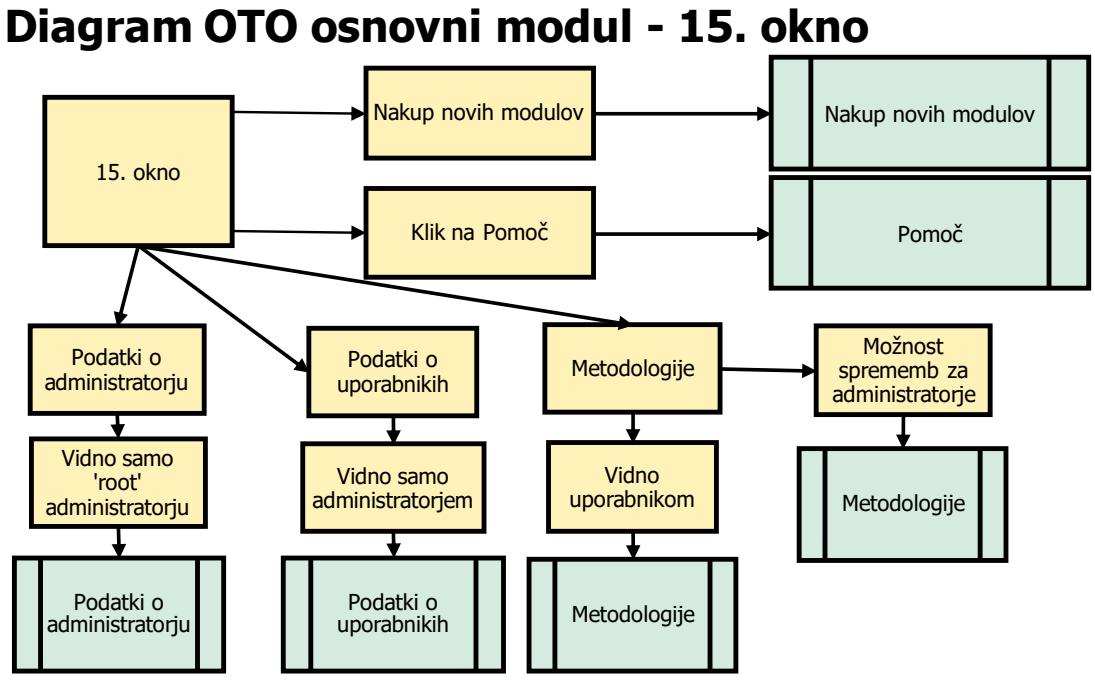
(b) Podatki o administratorju – določi se, kdo bo administrator (osnovni podatki ob nakupu /demo so že vpisani). Podatke lahko administrator spreminja, obstajati pa mora še nadadministrator, do katerega dostopa samo razvijalec.

(c) Podatki o uporabnikih – določi se vse uporabnike aplikacije (kdo bo imel dostop, kakšne vrste dostop (omejitve po modulih).

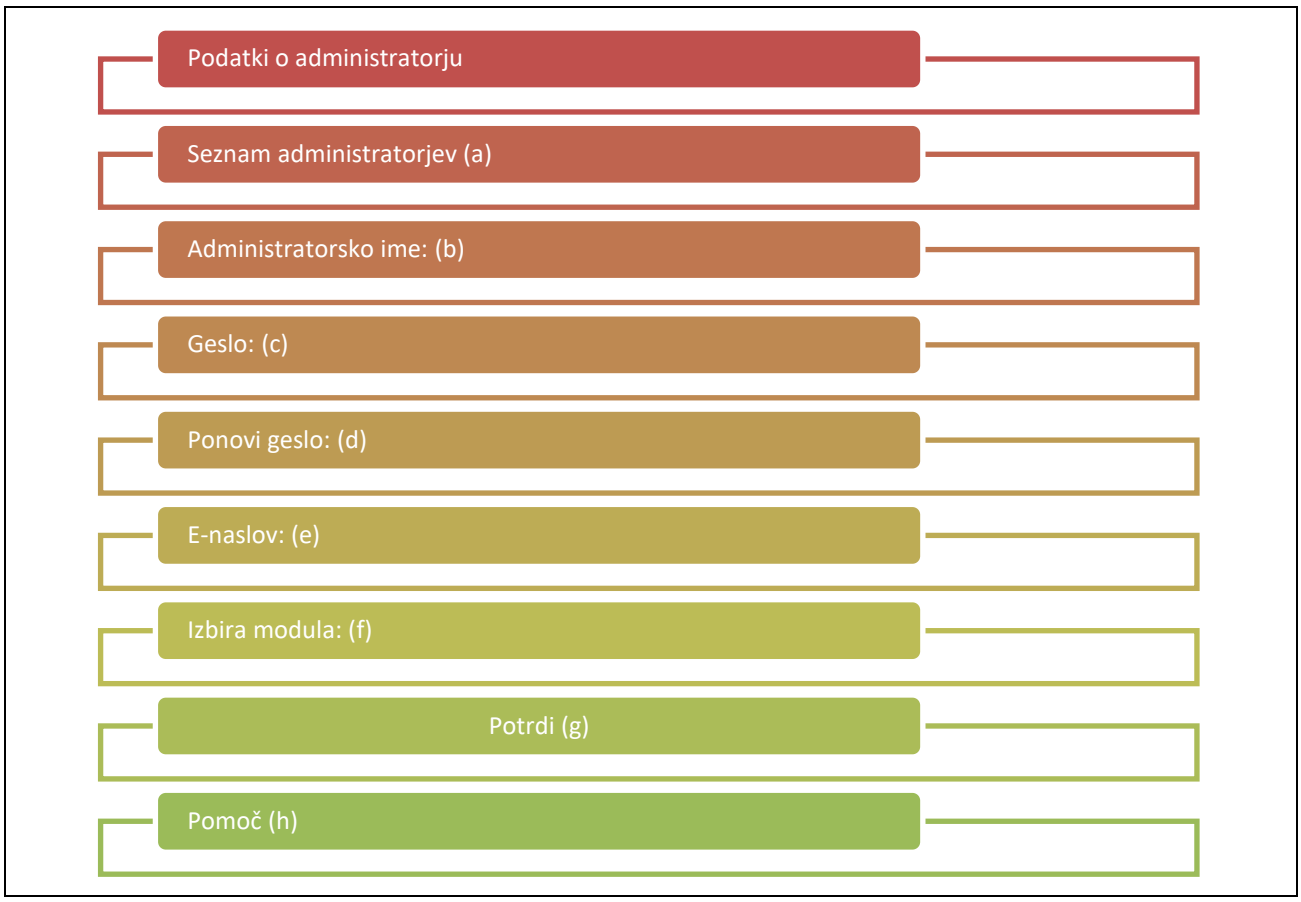
(d) Metodologije ocene tveganja – to so že določene metodologije z opisom vseh njihovih podatkov in povezavi na posamezen modul. Tu je prikazana možnost dodajanja metodologij (spremembe v matriki ali celotnih katalogih nevarnosti, vplivih in posledicah).

(e) Nakup novih ocen tveganja – to je povezava na spletno stran, kjer dobimo podatke o uporabniku (od kod dostopa, da se lahko personalizira nakup).

(f) Pomoč – je opis vseh aktivnosti in načina uporabe aplikacije.



Slika 48: 15. diagram aktivnosti OTO



Slika 49: 16. pojavno okno OTO

Administratorji aplikacije lahko vidijo seznam vseh administratorjev, vendar je možno upravljati s posameznimi administratorji samo preko nadrejenega (root) administratorja.

(a) Seznam vseh administratorjev aplikacije, vključno z nadrejenim (root), ki se ga ne da brisati, in katerega dobi stranka ob nakupu aplikacije. Nadrejenega (root) administratorja se ne da spreminjati. V seznamu se lahko tudi briše administratorjeve račune, vendar samo, če jih je administrator sam ustvaril. Nadrejeni (root) administrator lahko briše vse, razen svojega računa.

(b) Uporabniško ime za vpis novega administratorja. Najmanj 3 znaki.

(c) Geslo za vpis novega administratorja.

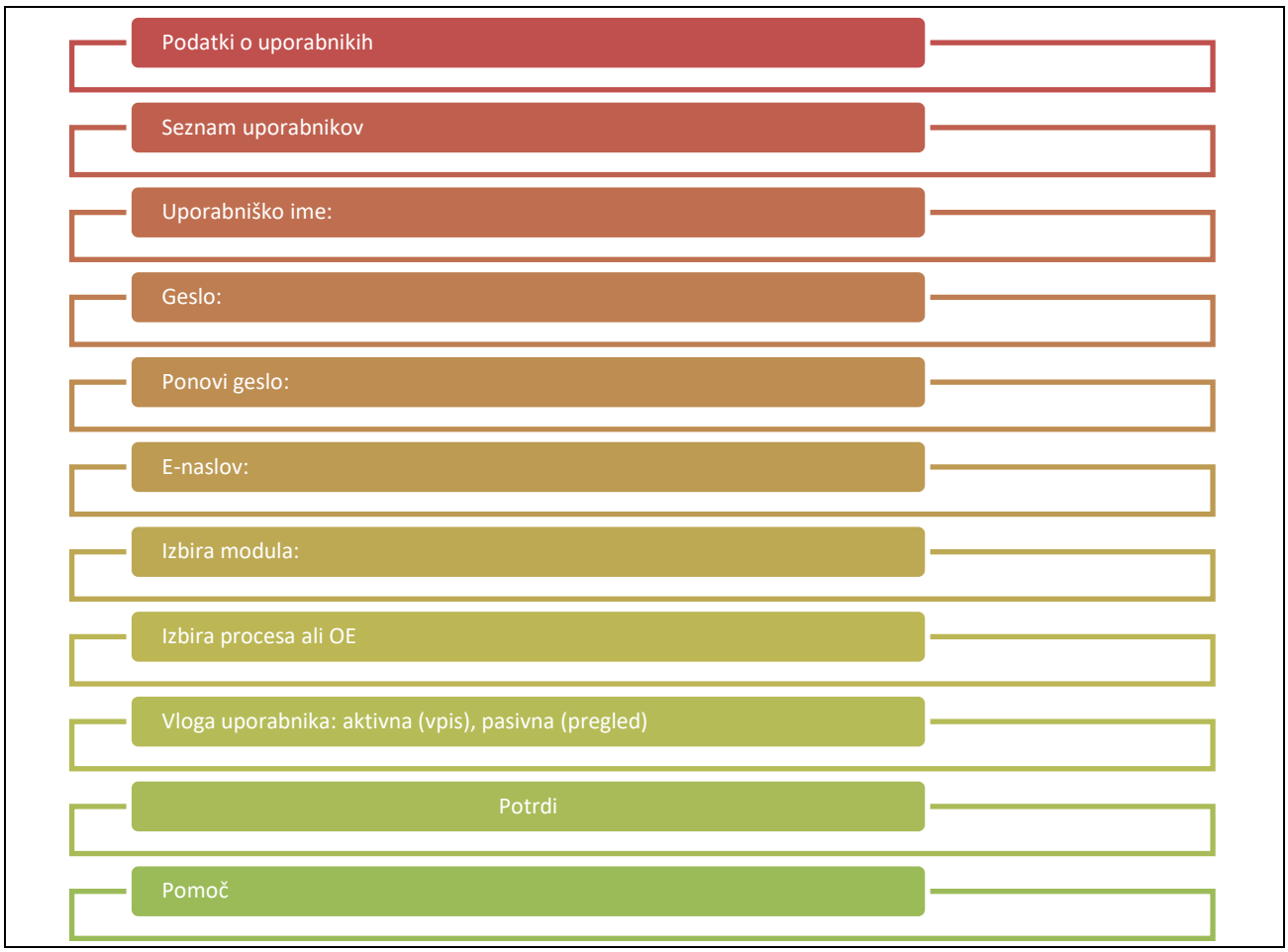
(c) Geslo se ponovi, da ne pride do napak.

(d) E-naslov je pomemben zaradi obvestil poslanih po e-pošti (ukrepi, obvestila o preteku rokov, kreiranje novega administratorja). Obvestilo o novem administratorju pride tako na naslov kreiranega administratorja, kot tudi na naslov tistega, ki ga kreira. Nadrejeni (root) administrator dobi e-naslov ob vpisu in nakupu aplikacije.

(f) Izbira modula pomeni, do katerega modula bo lahko administrator dostopal oziroma ga upravljal - lista vseh kupljenih modulov.

(g) Potrdi - potrditev vpisanih podatkov.

(f) Pomoč – opis vseh aktivnosti in načina vpisa ali izbrisa administratorjev.



Slika 50: 17. pojavno okno OTO

Administratorji aplikacije lahko vidijo seznam vseh uporabnikov, možno jih je upravljati s posameznimi uporabniki.

V seznamu se lahko tudi briše uporabnike, vendar to lahko naredi le administrator (glede na modul, kjer ima uporabnik pravice).

Geslo se ne bo omejevalo.

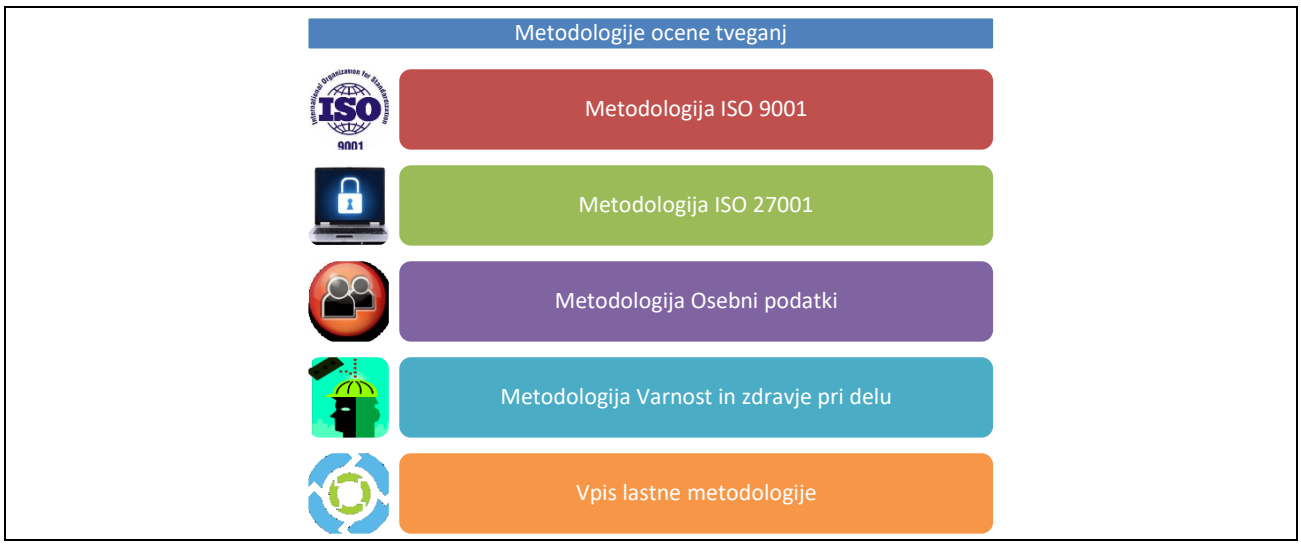
E-naslov je pomemben zaradi obvestil, poslanih po e-pošti (ukrepi, obvestila o preteku rokov, kreiranje novega uporabnika).

Izbira modula pomeni, do katerega modula bo lahko uporabnik lahko dostopal oziroma ga upravljal.

Izbira procesa ali OE pomeni, do katerega procesa ali OE bo lahko dostopal.

Vloga uporabnika pomeni, ali bo lahko ocenjeval tveganja ali pa bo lahko dobil samo ukrepe za izvedbo.

Pomoč – je opis vseh aktivnosti in način uporabe aplikacije.



Slika 51: 18. pojavno okno OTO

Vse metodologije so vezane na matriko:

		Posledice (Y os)					
		Y1	Y2	Y3	Y4	Y5	Y6
Verjetnost (X os)	X1	T2	T3	T4	T5	T5	T5
	X2	T2	T3	T3	T4	T5	T5
	X3	T1	T2	T3	T4	T4	T5
	X4	T1	T2	T3	T3	T4	T5
	X5	T1	T1	T2	T3	T4	T4

Slika 52: Matrika ocenjevanja tveganj OTO

X in Y os, s tem, da se osi ne smeta omejevati (Xn, Yn). Na X os se bo nanašala verjetnost uresničitve grožnje, ki jo lahko opišemo z več komponentami (časovno, odstotkovno, opisno), kar je možno vpisati ob posameznem elementu X osi. Na primer:

X1 = 1x na dan, 20 %, zelo verjetno (glej primer zgoraj) – odvisno od posamezne grožnje v posameznem modulu (glede na grožnjo, npr. požar v proizvodnji).

Če vzamemo modul ISO 9001, bo npr. v procesu proizvodnje (ki bo vsebovala objekte: OE Proizvodnja, delovna sredstva, zaposlene in stavba na Delavski cesti 1) ocena tveganja narejena tako, da bo sledilo vprašanje:

Ali je povečana možnost požara v proizvodnji?

X1 – Da, vnetljive snovi, pomanjkljivo izvajanje požarne varnosti.

X2 – Da, ni vnetljivih snovi, pomanjkljivo izvajanje požarne varnosti.

X3 – Ne, vnetljive snovi, ustrezno izvajanje požarne varnosti (gasilniki, usposobljeni zaposleni).

X4 – Ne, vnetljive snovi, ustrezno izvajanje požarne varnosti (protipožarni sistem, alarm, gasilniki, usposobljeni zaposleni).

X5 – Ne, ni vnetljivih snovi, ustrezno izvajanje požarne varnosti (gasilniki, usposobljeni zaposleni).

Posamezen odgovor se veže avtomatično na X os (X1, X2, X3, X4, X5 …)

Na Y os se bodo razvrščale posledice uresničitve grožnje na poslovanje, kar bo pomenilo aktivnost, ki je odvisna od tipa vira (tip objekta).

Y1 = poškodba opreme, poškodba ljudi, nedelovanje informacijske infrastrukture, itd. (glej primer zgoraj) – odvisno je od posamezne grožnje v posameznem modulu (glede na grožnjo, npr. požar v proizvodnji).

Kakšne so posledice požara v proizvodnji?

Y1 – Ni zaznane škode.

Y2 – Manjša zaznana škoda.

Y3 – Krajši izpad poslovnega procesa.

Y4 – Manjša škoda na opremi, krajši izpad poslovnega procesa.

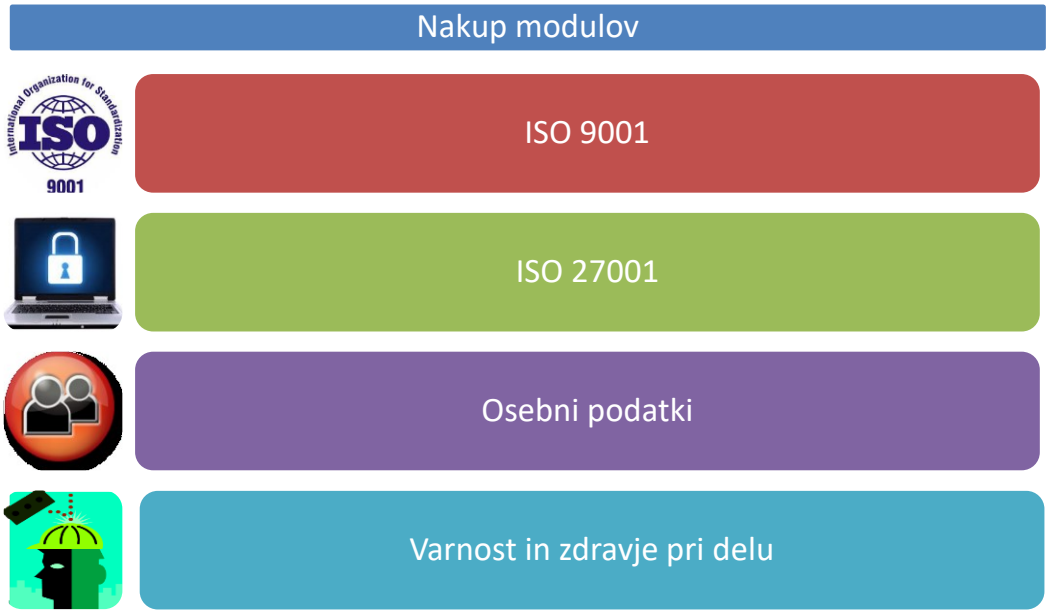
Y5 – Večje poškodbe opreme, poškodbe ljudi, zaustavitev poslovnega procesa.

Y6 – Uničenje opreme, izguba življenja ljudi, zaustavitev poslovnega procesa.

Posamezen odgovor se avtomatično nanaša na Y os (Y1, Y2, Y3, Y4, Y5 …)

Avtomatično se izračuna tveganje:

Xn x Yn = Tn



Slika 53: 19. pojavno okno OTO

Nakup novih modulov in ostale informacije bodo objavljene na spletni strani, do katere bo možen dostop s klikom na nakup modulov.

Slika 54: 20. pojavno okno OTO

Pomoč – je opis vseh aktivnosti in način uporabe aplikacije.

6.3.2 Seznam tabel v podatkovni bazi

OTO osnovne tabele

T_OBJECT tabela, ki predstavlja osnovne objekte v drevesu, med seboj so povezljivi kot nasledniki

OBJECT_ID	NUM SEQUENCE	enolični ključ zapisa
OBJECT_TYPE_ID	NUM	tip objekta
OBJECT	STRING	kratek opis objekta
OBJECT_DESC	STRING	dolg opis objekta
DATE_CREATED	TIMESTAMP	datum kreiranja objekta
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril objekt
STATUS	NUM (0/1)	1-delujoč, 0-nedelujoč
DATE_STATUS	TIMESTAMP	datum spremembe statusa
USER_ID_STATUS	NUM	uporabnik, ki je spremenil status

T_OBJECT_OWNER tabela lastnikov objektov, lastnik objekta je avtomatsko tudi lastnik vseh podrejenih objektov

OBJECT_ID	NUM	id objekta
OWNER_USER_ID	NUM	id lastnika objekta
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja lastnika
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril lastnika
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja lastnika
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl lastnika

T_OBJECT_TYPE tabela, ki predstavlja vse možne tipe objektov, je preddefinirana z vrednostmi, uporabnik sam lahko tudi dodaja svoje tipe, vendar novo dodani tipi niso upoštevani v metodologijah

OBJECT_TYPE_ID	NUM SEQUENCE	enolični ključ zapisa
OBJECT_TYPE	STRING	opis tipa objekta
DATE_CREATED	TIMESTAMP	datum kreiranja tipa objekta
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril tip objekta
STATUS	NUM (0/1)	1-delujoč, 0-nedelujoč
DATE_STATUS	TIMESTAMP	datum spremembe statusa
USER_ID_STATUS	NUM	uporabnik, ki je spremenil status

T_OBJECT_TYPE_TYPE tabela, ki označuje, kateri tipi objektov so lahko nasledniki določenih tipov. Zaradi enostavnosti se pravilo obrne in tabela predstavlja tiste tipe, ki ne smejo biti nasledniki posameznih tipov.

OBJECT_ID	NUM	id objekta
OBJECT_TYPE_ID	NUM	id tipa objekta
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja pravila
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril pravilo
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja pravila
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl pravilo

T_OBJECT_PARM tabela, ki predstavlja vse možne parametre na posameznem objektu. Tipi parametrov so preddefinirani, uporabnik sam lahko tudi dodaja svoje parametre, vendar novo dodani parametri niso upoštevani v metodologijah

OBJECT_PARM_ID NUM	SEQUENCE	enolični ključ zapisa
OBJECT_PARM	STRING	opis parametra

Če lahko predpostavimo, da imajo vsi parametri vrednost v numeriki, naslednje polje ni potrebno:

OBJEVT_PARM_TYPE	NUM(0/1)	0-num, 1-string
DATE_CREATED	TIMESTAMP	datum kreiranja parametra
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril parameter
STATUS	NUM (0/1)	1-delujoč, 0-nedelujoč
DATE_STATUS	TIMESTAMP	datum spremembe statusa
USER_ID_STATUS	NUM	uporabnik, ki je spremenil status

T_OBJECT_TYPE_PARM tabela, ki pove, kateri parametri se lahko vežejo na posamezne tipe objektov. Zaradi poenostavitve ponovno obrnemo in vpišemo samo prepovedane.

OBJECT_TYPE_ID	NUM	id tipa objekta
OBJECT_PARM_ID	NUM	id parametra
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja pravila
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril pravilo
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja pravila
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl pravilo

T_PARM_OBJECT_TYPE tabela pove, katere tipe objektov ima lahko posamezen parameter kot soodvisne oz., kateri objekt vpliva na sam parameter, čeprav ta objekt ni neposredno povezan z objektom, na katerem je parameter.

OBJECT_PARM_ID	NUM	id parametra
OBJECT_TYPE_ID	NUM	id tipa objekta
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja pravila
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril pravilo
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja pravila
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl pravilo

T_OBJECT_PARMS tabela, ki pove, katere parametre ima posamezen objekt in vrednosti teh parametrov

OBJECT_PARMS_ID	NUM	SEQUENCE	enolični ključ zapisa
OBJECT_ID	NUM		id objekta
OBJECT_PARM_ID	NUM		id parametra

Če lahko predpostavimo, da imajo vsi parametri vrednost v numeriki, je potrebno le naslednje polje:

PARM_VALUE	NUM	vrednost parametra

V nasprotne primeru pa potrebujemo dve polji.

PARM_VALUE_NUM	NUM	numerična vrednost polja
PARM_VALUE_STRING	STRING	string vrednost parametra
VALID_FROM	TIMESTAMP	datum začetka vrednosti
DATE_CREATED	TIMESTAMP	datum kreiranja vrednosti
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril vrednost
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl vrednost

T_OBJECT_PARM_OBJECT tabela soodvisnih objektov na posameznem parametru objekta

OBJECT_PARMS_ID	NUM	enolični ključ zapisa
OBJECT_ID	NUM	id soodvisnega objekta
VALID_FROM	TIMESTAMP	datum začetka soodvisnosti

DATE_CREATED	TIMESTAMP	datum kreiranja soodvisnosti
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril soodvisnost
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl soodvisnost

T_OBJECT_OBJECT tabela, ki predstavlja povezanost med objekti

OBJECT_ID	NUM	id objekta tipa starši
ANC_OBJECT_ID	NUM	id objekta tipa naslednik
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja povezave
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril povezavo
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl objekt

T_PROCESS tabela, ki predstavlja procese

PROCESS_ID	NUM SEQUENCE	enolični ključ zapisa
PROCESS	STRING	kratek opis procesa
PROCESS_DESC	STRING	dolg opis procesa
DATE_CREATED	TIMESTAMP	datum kreiranja procesa
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril proces
STATUS	NUM (0/1)	1-delujoč, 0-nedelujoč
DATE_STATUS	TIMESTAMP	datum spremembe procesa
USER_ID_STATUS	NUM	uporabnik, ki je spremenil status

T_PROCESS_OWNER tabela prikazuje lastnike procesov, lastnik procesa je avtomatsko tudi lastnik vseh notranjih procesov

PROCESS_ID	NUM	id procesa
OWNER_USER_ID	NUM	id lastnika procesa
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja lastnika
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril lastnika
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja lastnika
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl lastnika

T_PROCESS_PROCESS tabela, ki prikaže, katere procese vsebuje posamezen proces

PROCESS_ID	NUM	id proces, ki vsebuje druge procese
SLAVE_PROCESS_ID	NUM	id vsebovanega procesa
VALID_FROM	IMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja vsebovanosti
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril vsebovanost
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja vsebovanosti
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl vsebovanost

T_PROCESS_START_END tabela kaže na začetek in konec procesa

PROCESS_ID	NUM	id procesa
START_OBJECT_ID	NUM	id začetnega objekta
END_OBJECT_ID	NUM	id končnega objekta
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja

USER_ID_CREATED	NUM	uporabnik, ki je ustvaril zapis
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja zapisa
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl zapis

T_PROCESS_OBJECT	tabela, ki kaže, katere objekte vsebuje proces	
PROCESS_ID	NUM	id procesa
OBJECT_ID	NUM	id vsebovanega objekta
VALID_FROM	TIMESTAMP	datum začetka veljavnosti
DATE_CREATED	TIMESTAMP	datum kreiranja
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril zapis
VALID_TO	TIMESTAMP	datum konca veljavnosti
DATE_FINISHED	TIMESTAMP	datum zaprtja zapisa
USER_ID_FINISHED	NUM	uporabnik, ki je zaprl zapis

T_OBJECT_DOCUMENT	tabela za dokumente vezane na objekt	
OBJECT_DOCUMENT_ID	NUM SEQUENCE	enolični ključ zapisa
OBJECT_ID	NUM	id objekta
DOC_TYPE	NUM	tip dokumenta; 0-v bazi, 1-povezava na dokument
DOC_DESC	STRING	opis, ime dokumenta
DOCUMENT	BLOB	dokument v bazi, če je DOC_TYPE=0
DOC_PATH	STRING	kazalec na dokument, če je DOC_TYPE=1
DATE_CREATED	TIMESTAMP	datum kreiranja dokumenta
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril dokument
STATUS	NUM (0/1)	1-delujoč, 0-nedelujoč
DATE_STATUS	TIMESTAMP	datum spremembe dokumenta
USER_ID_STATUS	NUM	uporabnik, ki je spremenil status

T_PROCESS_DOCUMENT	tabela za dokumente vezane na objekt	
PROCESS_DOCUMENT_ID	NUM SEQUENCE	enolični ključ zapisa
PROCESS_ID	NUM	id procesa
DOC_TYPE	NUM	tip dokumenta; 0-v bazi, 1-povezava na dokument
DOC_DESC	STRING	opis, ime dokumenta
DOCUMENT	BLOB	dokument v bazi, če je DOC_TYPE=0
DOC_PATH	STRING	kazalec na dokument, če je DOC_TYPE=1
DATE_CREATED	TIMESTAMP	datum kreiranja dokumenta
USER_ID_CREATED	NUM	uporabnik, ki je ustvaril dokument
STATUS	NUM (0/1)	1-delujoč, 0-nedelujoč
DATE_STATUS	TIMESTAMP	datum spremembe dokumenta
USER_ID_STATUS	NUM	uporabnik, ki je spremenil status

7 Ostale zahteve glede delovanja programske opreme

7.1 Zahteve časovnega osveževanja

Zahteve delovanje so naslednje:

- Posamezna sprememba se mora avtomatično shraniti.
- Čas zapisa spremembe v bazo ne sme biti daljši od 2 sekund.
- Čas prikaza posamezne ocene tveganja ne sme biti daljši od 4 sekund.
- Čas izpisa posameznega elementa ne sme biti daljši od 10 sekund.

- V primeru hkratnih vnosov več uporabnikov se morajo spremembe prikazovati vsem oziroma morajo biti obveščeni o možnih spremembah.

7.2 Zahteve zaščite in varnosti programske opreme

Zahteve zaščite in varnosti so naslednje:

- Vsak uporabnik ima svoje uporabniško ime (in geslo).
- Posamezen uporabnik ima eno izmed določenih vlog.
- Možen je izpis podatkov kot varnostna kopija.

7.3 Atributi kakovosti programske opreme

Zahteve kakovosti so naslednje:

- Programska oprema mora zagotavljati možnost nadgradnje (tehnične in vsebinske) preko zunanjih povezav (nameščanje preko spletne povezave).
- Programska oprema mora zagotavljati možnost prijave napak.

8 Sklepne ugotovitve

8.1 Nujnost ocenjevanja tveganj

Ocenjevanje tveganj je smiselno izvajati ne samo zaradi zahtev zakonodaje in standardov, pač pa predvsem zaradi izboljšanja poslovanja. Organizacije bi zato morale opredeliti, kaj vse spada v obseg ocenjevanja tveganj in na podlagi tega začeti proces celovitega obvladovanja tveganj. Ob tem se je potrebno zavedati, da je zaradi pomanjkanja napotkov glede tehnik ocenjevanja tveganj (metodologij) potrebno to področje natančno opredeliti v sami organizaciji. Organizacije se lahko najbolje pripravijo na ocenjevanje tveganj, če sledijo dobrim praksam standardov. V vse aktivnosti priprave ocene tveganja naj vključijo čim več ključnih oseb – poslovodstva ter vodje organizacijskih enot oziroma skrbnikov poslovnih procesov in sistemov vodenja. Ravno s tem namenom, da bi organizacijam pomagala pri izboljševanju poslovanja, je nastala programska oprema OTO. Ker je težko in časovno zamudno ocenjevati tveganja, je programska podpora tovrstnemu odločanju bistvena za uspešno zmanjševanje previsokih tveganj in znižanje stroškov tega procesa. S tem pa se poveča konkurenčnost organizacij na trgu.

8.2 Tehnike ocenjevanja tveganj (metodologije)

Vprašati se je potrebno, kako se odločiti za primerno metodologijo ocenjevanja tveganj. Predstavljena je bila matrika posledic in verjetnosti (Consequence/probability matrix) zaradi svoje enostavnosti in podatkov, ki so ključnega pomena za poslovodstvo. Katero metodologijo ocenjevanja tveganj bo neka organizacija uporabila, je odvisno od mnogih dejavnikov, mora pa pri tem upoštevati vse zahteve ocenjevanja tveganj (npr. nadzorni organi določajo, da se mora izvajati ocenjevanje tveganj po določeni metodologiji). Priporočil bi le, da se ocenjevanje tveganj na več področjih med seboj povezuje vsaj na področju definiranja ukrepov, ko se predstavi ugotovitve vseh ocen tveganj v organizaciji in odloči za smiselne (lahko tudi skupne) ukrepe za izboljševanje poslovanja.

8.3 Organizacije in ocenjevanje tveganj

Čim večja je organizacija, tem kompleksnejše bo obvladovanje (in s tem ocenjevanje) tveganj. Pri tem se je potrebno zavedati, da z velikostjo organizacije raste tudi število oseb, ki so vključene v ocenjevanje tveganj, kar pomeni, da bo potrebno izbirati med tehnikami ocen tveganj, ki omogočajo dokaj uniformiran pristop znotraj organizacije. S tem se bodo nivoji tveganj določali smiselno po vseh organizacijskih enotah oziroma poslovnih procesih in ne bo težav z različnim razumevanjem ocenjevanja tveganj. Nujno za vse organizacije, ne glede na panogo ali velikost, pa je, da se ocenjevanja tveganj lotijo z uporabo dobrih praks in da ocene tveganja ne jemljejo kot administrativni postopek, ki mora biti opravljen zaradi zahtev nadzornikov ali inšpekcije.

Obvladovanje (in s tem ocenjevanje) tveganj je za organizacije nekaj, kar je že potrebno izvajati oziroma bo poudarek na mehanizmu obvladovanja tveganj v naslednjih letih še rastel. Kako se bo to izvajalo, pa je odvisno od tega, ali želimo z uporabo tega mehanizma dobiti podatke, ki nam bodo pomagali pri vodenju in izboljševanju poslovanja. Tako kot pri sistemih vodenja, je tudi pri obvladovanju tveganj najbolj pomembno podprtje poslovodstva.

Če pa imamo podporo poslovodstva, je potrebno znati integrirati vse ocene tveganja v organizaciji, da bomo lahko enostavno in razumljivo to prikazali vsem ključnim osebam v organizaciji in od njih dobili predloge ukrepov, ki bodo celovito pomagali pri poslovanju.

Enostavna in razumljiva ocena tveganja, ki temelji na ustreznih kvantitativnih in kvalitativnih merilih, je zato cilj, ki ga poskušam doseči. Ker je hkrati ocena tudi ustrezno podprta s programsko opremo, lahko OTO postane orodje, ki ga bodo z veseljem uporabljali vsi, ki si želijo izboljšati delovanje in konkurenčnost organizacije.

9 Priloge

- programska oprema OTO, verzija 1.0
- metodologija ISO 9001
- metodologija ISO/IEC 27001

10 Seznam uporabljenih virov

1. ISO 31000:2011, www.iso.org, 25.8.2014
2. ISO/TR 31004:2013, www.iso.org, 25.8.2014
3. ISO 31010:2011, www.iso.org, 25.8.2014
4. http://www.siq.si/ocenjevanje_sistemov_vodenja/, 25.8.2014
5. Anderson, Chris. How to Build Effective Management Systems, Bizmanualz, January 26, 2005.
6. http://www.iso.org/iso/home/standards/management-standards.htm, 25.8.2014
7. www.bsigroup.com, 25.8.2014
8. ISO/IEC 27001:2013, www.iso.org, 25.8.2014
9. PCI-DSS, www.pcisecuritystandards.org/security_standards/, 25.8.2014
10. Zakon o varstvu osebnih podatkov (ZVOP-1), UL št. 94, 16.10.2007
11. Zakon o tajnih podatkih (ZTP), UL št. 50, 16.05.2006
12. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA-A), UL št. 51, 07.07.2014
13. Enotne tehnološke zahteve 2.1, II. Del, 10.07.2013
14. Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, UL št. 48, 01.06.2007
15. Zakon o elektronskih komunikacijah (ZEKOM-1), UL št. 109, 31.12.2012
16. ISO 9001:2015, www.iso.org, 25.2.2016
17. ISO/IEC 27005:2011, www.iso.org, 25.8.2014
18. http://www.enisa.europa.eu/activities/risk-management, 25.8.2014
19. NIST 800-30 (01-2012), www.nist.gov, 25.8.2014
20. https://www.ip-rs.si/novice/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov-1365/, 17.5.2016
21. ISO/IEC Guide 73:2009 (2009). Risk management — Vocabulary. International Organization for Standardization, www.iso.org, 25.8.2014
22. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management, 13.6.2014
23. http://www.pisrs.si/Pis.web/pregledPredpisa?id=AKT_864, 25.11.2015
24. https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html, 10.4.2016
25. Taleb, Nassim. The black swan: the impact of the highly improbable, 2010
26. Koubek, Anni. Priročnik ISO 9001:2015 : razumevanje in izvajanje novih zahtev, 2016
27. Novak, Rajko, Zozolly, Mihajlo, Pribaković-Borštnik, Ana, Žagar, Tatjana, Bizjak, Igor, Burnik, Tomaž, Kaštrun, Ruli, Kaker, Blanka, Seražin, Miloš, Hozjan, Martina. Smernice za presojanje zahtev standardov ISO 9001:2015 in ISO 14001:2015, 2016
28. Žele, Mina. Kako izvesti analizo tveganja, da bodo rezultati uporabni v praksi, Varnostni forum : vaš osebni svetovalec za varovanje informacij ISSN: 1581-9221.- Letn. 4, nov. 2008 (2008), str. 26-27